OIPE
FEB 08 2006
PATENT & TRADEMARK OFFICE

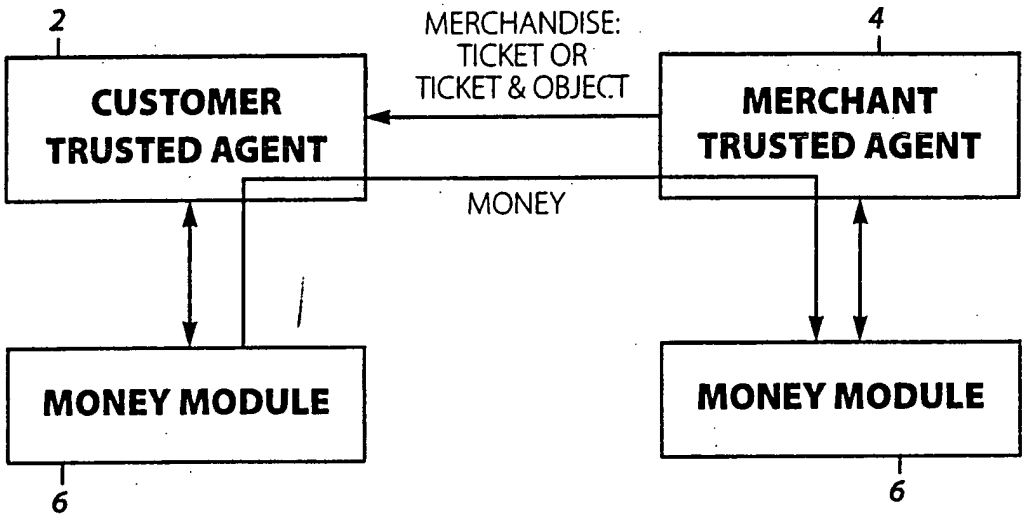

Figure 1

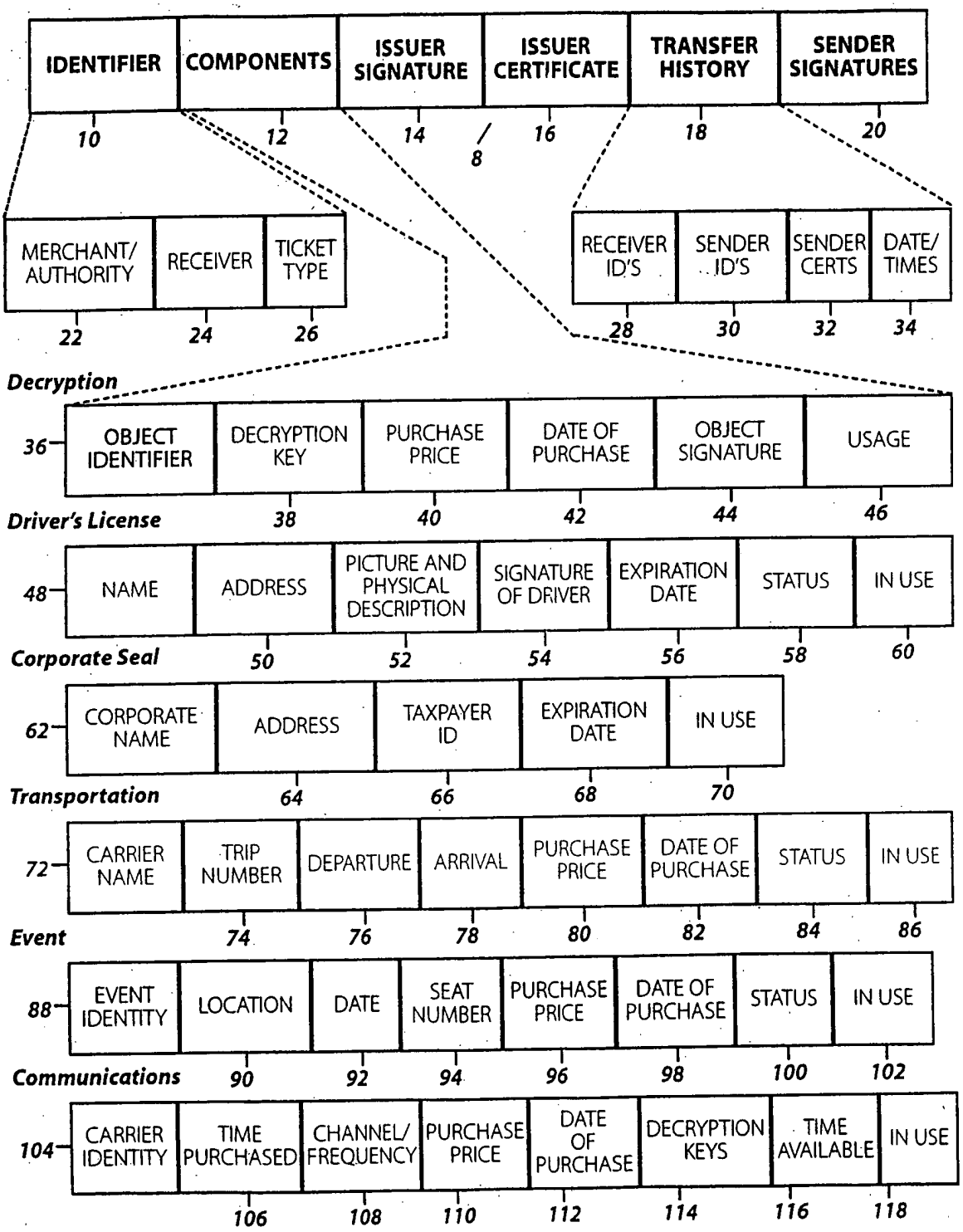
IDENTIFIER
COMPONENTS
ISSUER SIGNATURE
ISSUER CERTIFICATE
TRANSFER HISTORY
SENDER SIGNATURES
10
12
14
8
16
18
20
MERCHANT/ AUTHORITY
RECEIVER
TICKET TYPE
22
24
26
RECEIVER ID'S
SENDER ID'S
SENDER CERTS
DATE/ TIMES
28
30
32
34
Decryption
36
OBJECT IDENTIFIER
DECRYPTION KEY
PURCHASE PRICE
DATE OF PURCHASE
OBJECT SIGNATURE
USAGE
38
40
42
44
46
Driver's License
48
NAME
ADDRESS
PICTURE AND PHYSICAL DESCRIPTION
SIGNATURE OF DRIVER
EXPIRATION DATE
STATUS
IN USE
50
52
54
56
58
60
Corporate Seal
62
CORPORATE NAME
ADDRESS
TAXPAYER ID
EXPIRATION DATE
IN USE
64
66
68
70
Transportation
72
CARRIER NAME
TRIP NUMBER
DEPARTURE
ARRIVAL
PURCHASE PRICE
DATE OF PURCHASE
STATUS
IN USE
74
76
78
80
82
84
86
Event
88
EVENT IDENTITY
LOCATION
DATE
SEAT NUMBER
PURCHASE PRICE
DATE OF PURCHASE
STATUS
IN USE
90
92
94
96
98
100
102
Communications
104
CARRIER IDENTITY
TIME PURCHASED
CHANNEL/ FREQUENCY
PURCHASE PRICE
DATE OF PURCHASE
DECRYPTION KEYS
TIME AVAILABLE
IN USE
106
108
110
112
114
116
118

Figure 2

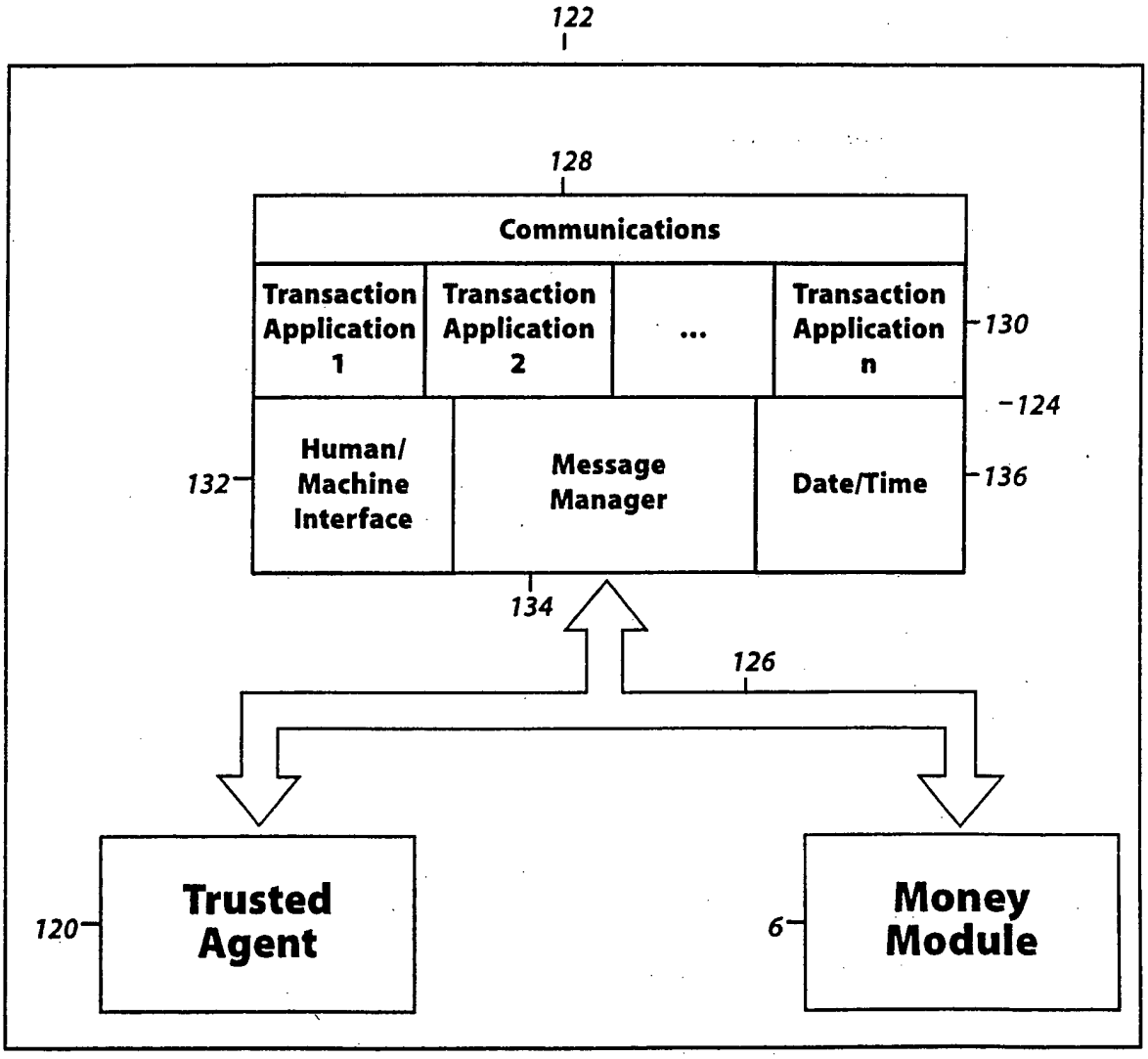
122
128
Communications
Transaction Application 1
Transaction Application 2
...
Transaction Application n
130
124
Human/ Machine Interface
132
Message Manager
Date/Time
136
134
126
Trusted Agent
120
Money Module
6

Figure 3

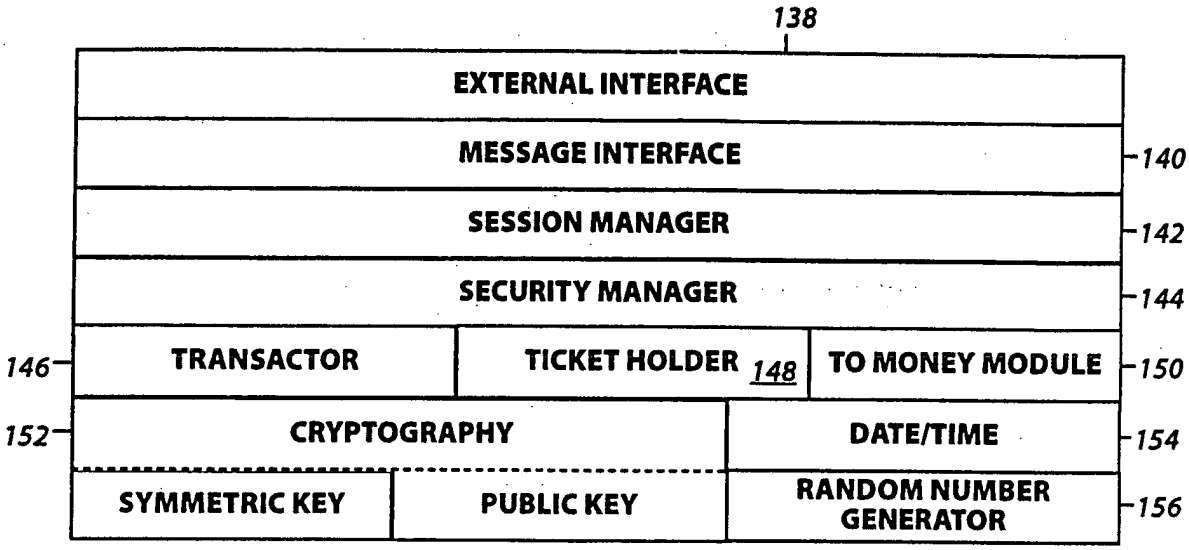

Figure 4A

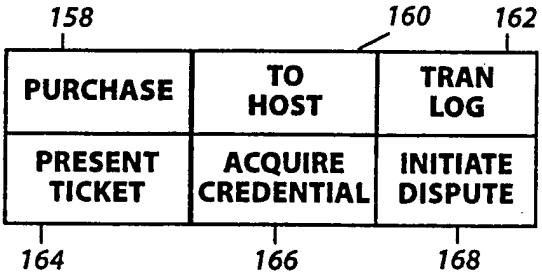

Figure 4B

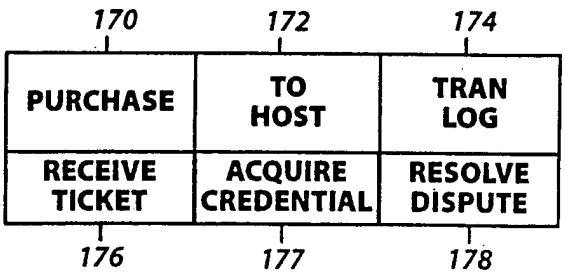

Figure 4C

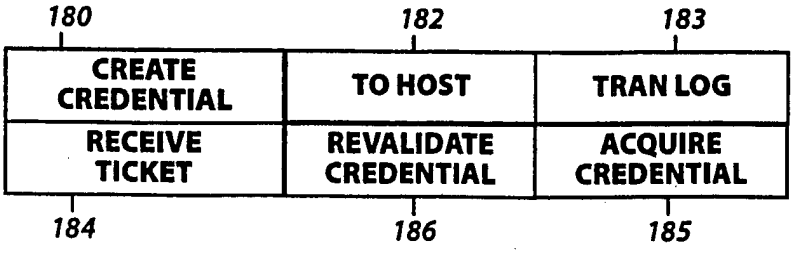

Figure 4D

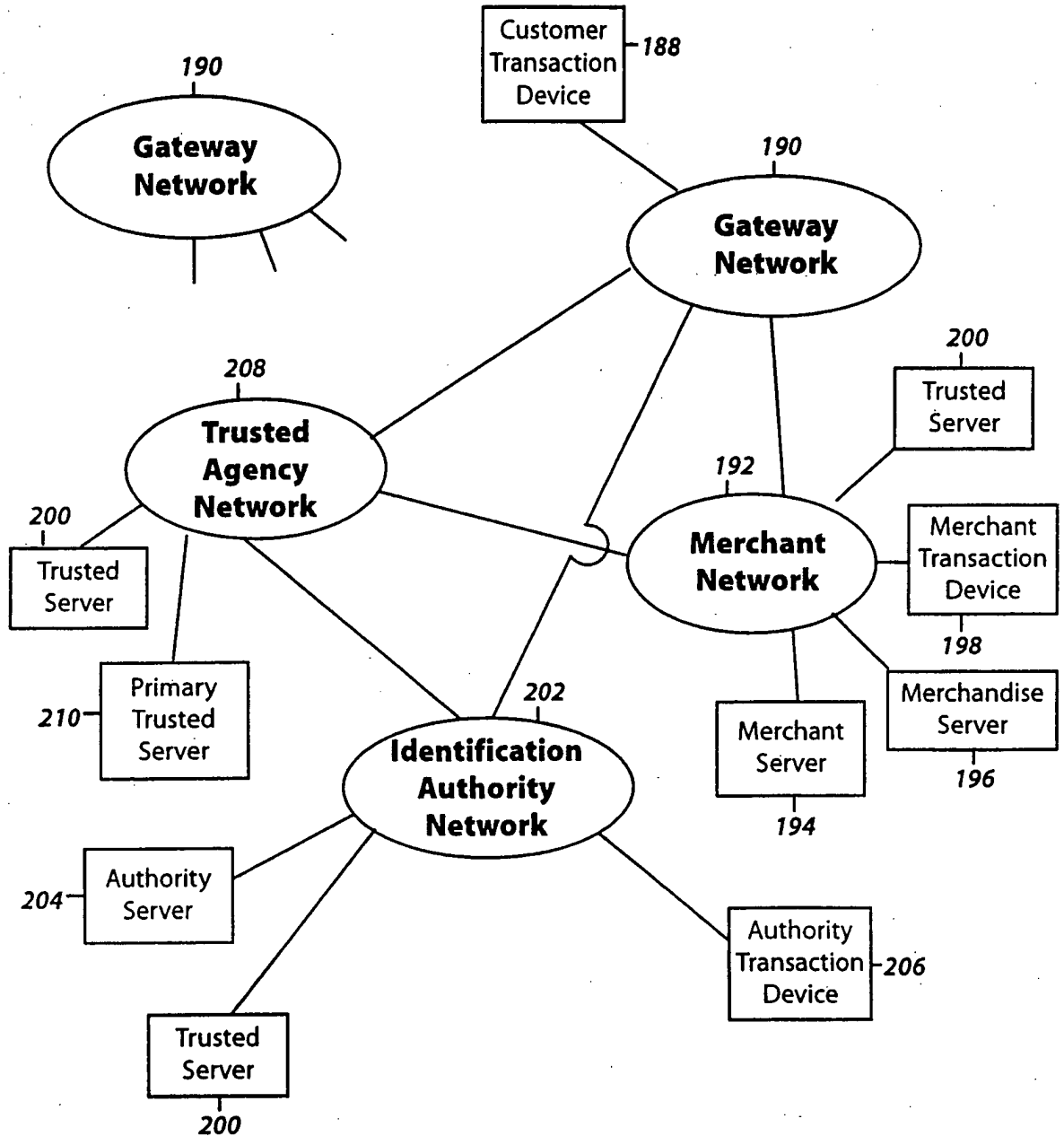
Customer Transaction Device
188
190
Gateway Network
190
Gateway Network
200
Trusted Server
208
Trusted Agency Network
192
200
Trusted Server
Merchant Network
Merchant Transaction Device
198
Merchandise Server
196
Primary Trusted Server
210
202
Identification Authority Network
Merchant Server
194
Authority Server
204
Authority Transaction Device
206
Trusted Server
200

Figure 5

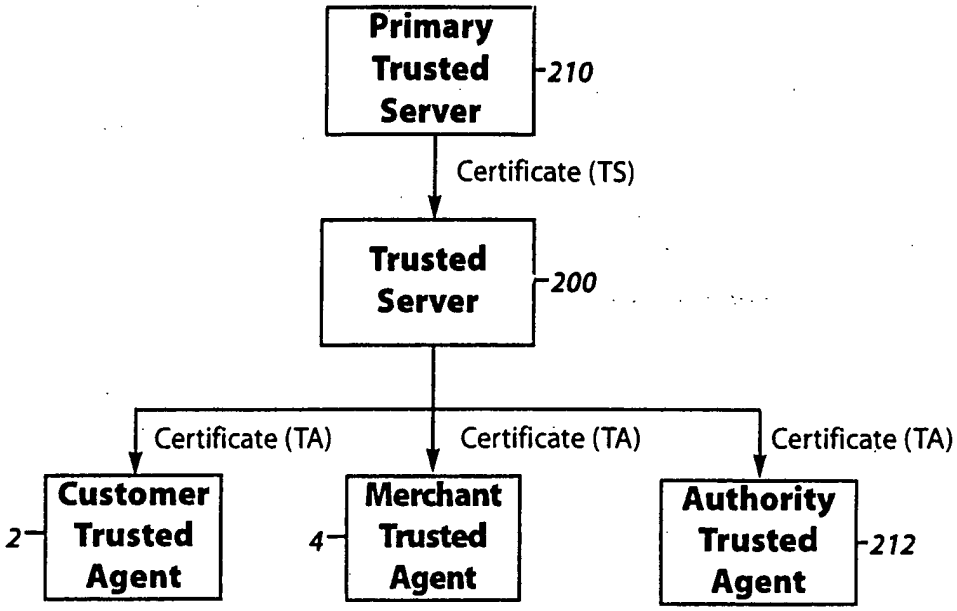

Figure 6A

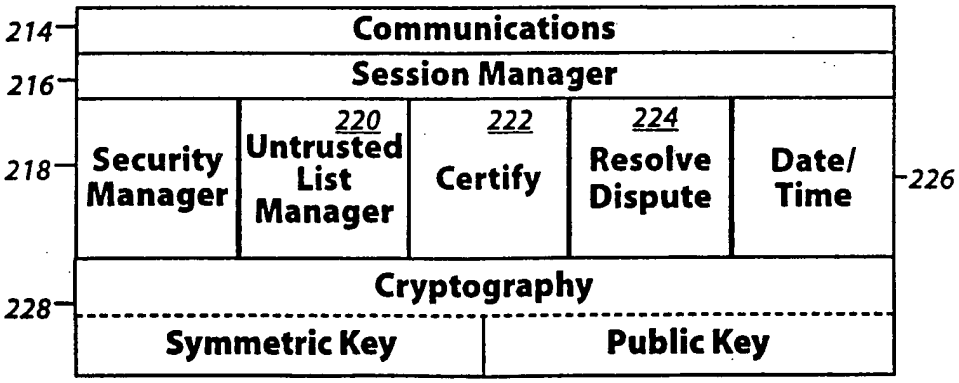

Figure 6B

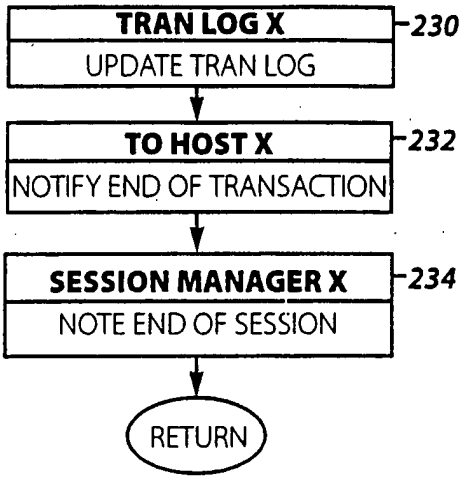

Figure 7A

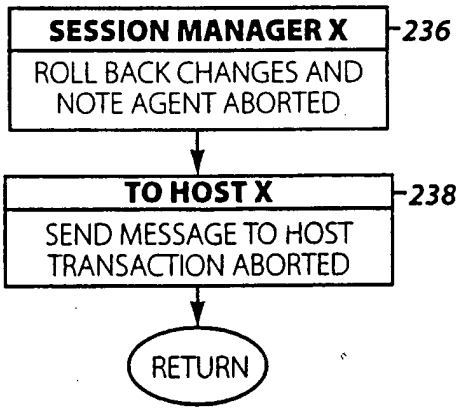

Figure 7B

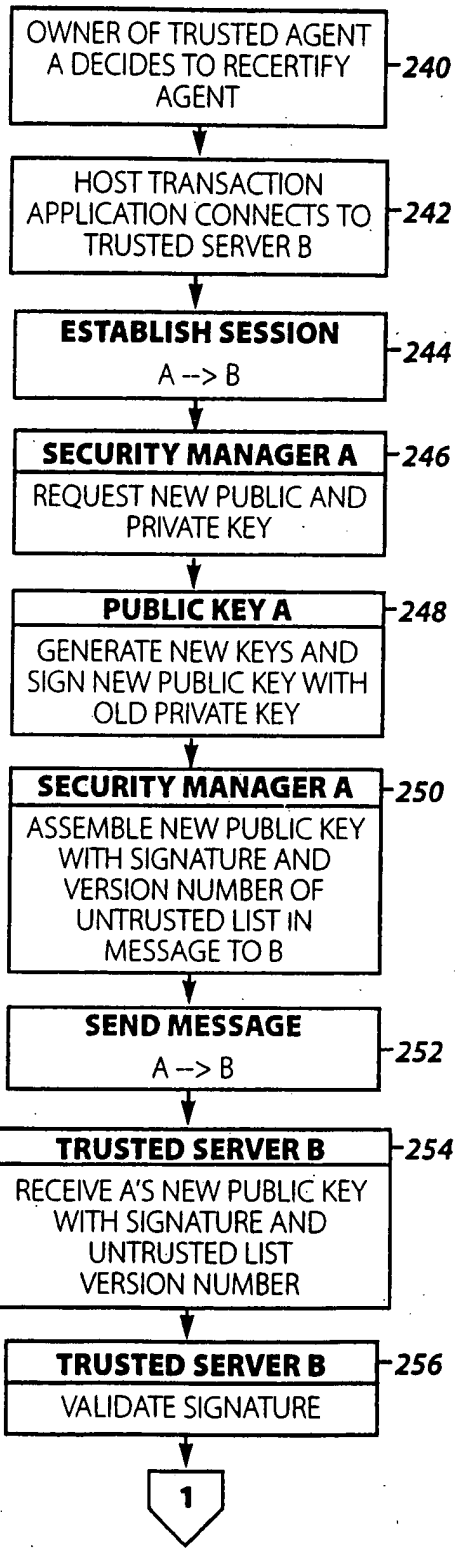
OWNER OF TRUSTED AGENT A DECIDES TO RECERTIFY AGENT
240
HOST TRANSACTION APPLICATION CONNECTS TO TRUSTED SERVER B
242
ESTABLISH SESSION
A --> B
244
SECURITY MANAGER A
REQUEST NEW PUBLIC AND PRIVATE KEY
246
PUBLIC KEY A
GENERATE NEW KEYS AND SIGN NEW PUBLIC KEY WITH OLD PRIVATE KEY
248
SECURITY MANAGER A
ASSEMBLE NEW PUBLIC KEY WITH SIGNATURE AND VERSION NUMBER OF UNTRUSTED LIST IN MESSAGE TO B
250
SEND MESSAGE
A --> B
252
TRUSTED SERVER B
RECEIVE A'S NEW PUBLIC KEY WITH SIGNATURE AND UNTRUSTED LIST VERSION NUMBER
254
TRUSTED SERVER B
VALIDATE SIGNATURE
256
1

Figure 8A

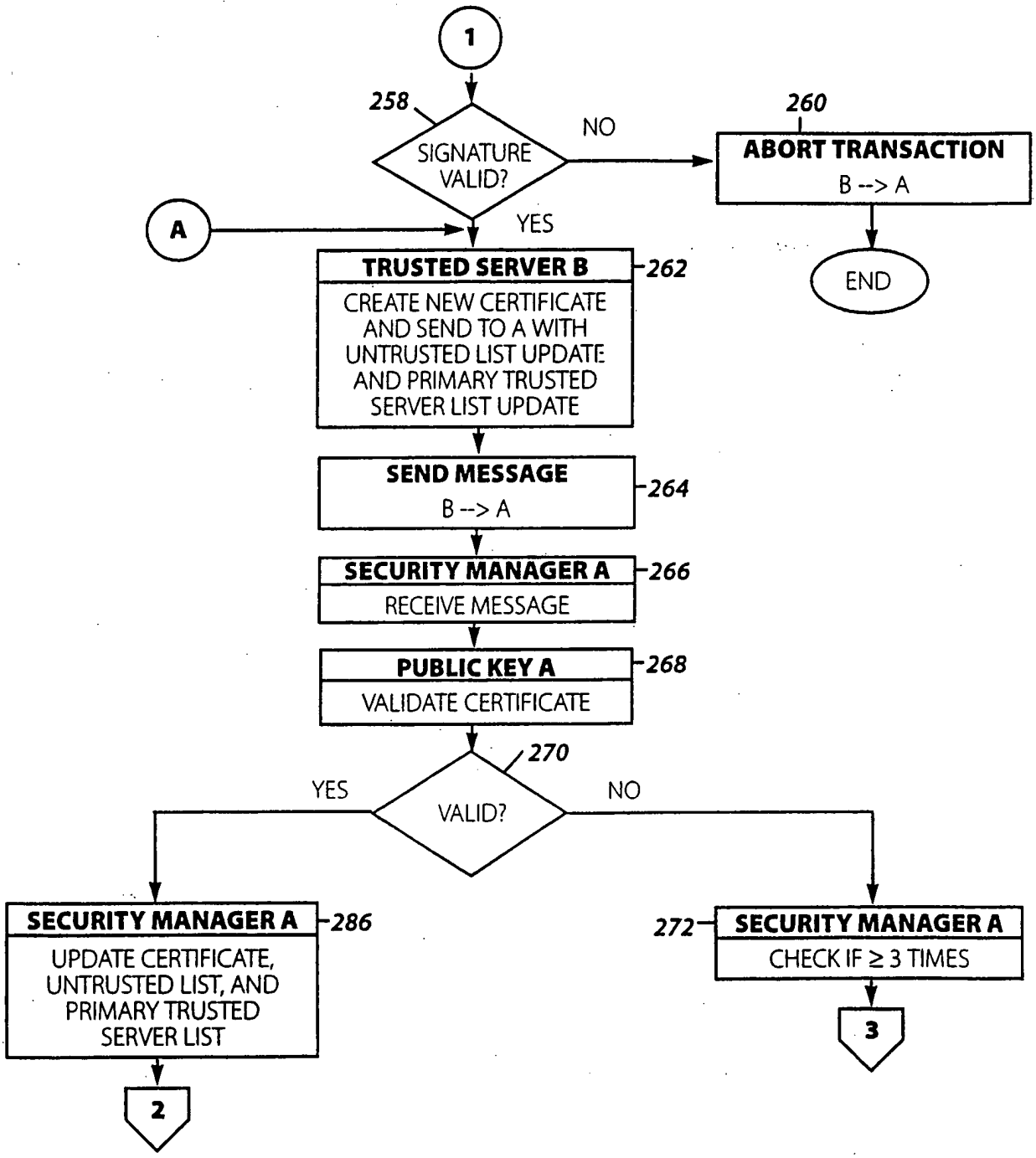
1
258
SIGNATURE VALID?
NO
260
ABORT TRANSACTION
B --> A
END
A
YES
TRUSTED SERVER B
262
CREATE NEW CERTIFICATE AND SEND TO A WITH UNTRUSTED LIST UPDATE AND PRIMARY TRUSTED SERVER LIST UPDATE
SEND MESSAGE
B --> A
264
SECURITY MANAGER A
266
RECEIVE MESSAGE
PUBLIC KEY A
268
VALIDATE CERTIFICATE
270
YES
VALID?
NO
SECURITY MANAGER A
286
UPDATE CERTIFICATE, UNTRUSTED LIST, AND PRIMARY TRUSTED SERVER LIST
2
272
SECURITY MANAGER A
CHECK IF ≥ 3 TIMES
3

Figure 8B

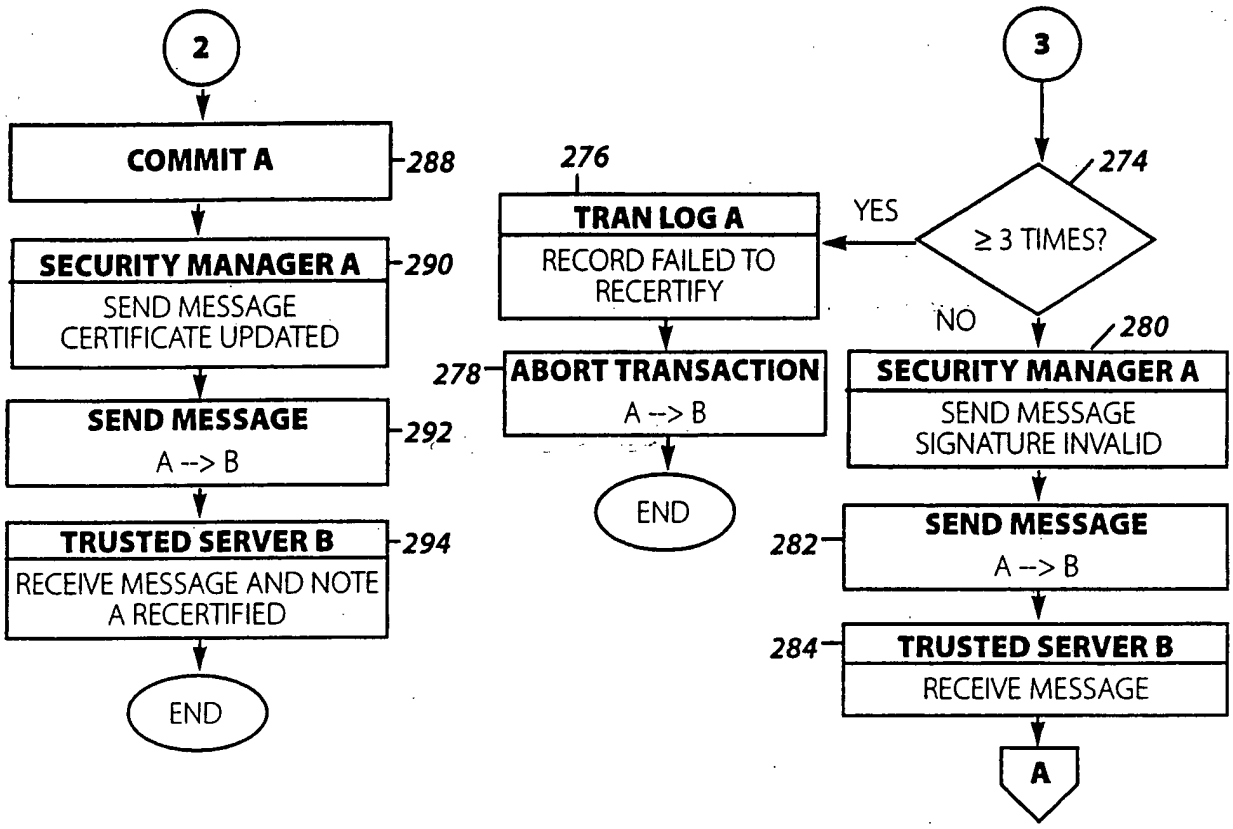
2
COMMIT A
288
SECURITY MANAGER A
290
SEND MESSAGE
CERTIFICATE UPDATED
SEND MESSAGE
292
A --> B
TRUSTED SERVER B
294
RECEIVE MESSAGE AND NOTE
A RECERTIFIED
END
3
274
≥ 3 TIMES?
YES
NO
276
TRAN LOG A
RECORD FAILED TO
RECERTIFY
278
ABORT TRANSACTION
A --> B
END
280
SECURITY MANAGER A
SEND MESSAGE
SIGNATURE INVALID
282
SEND MESSAGE
A --> B
284
TRUSTED SERVER B
RECEIVE MESSAGE
A

Figure 8C

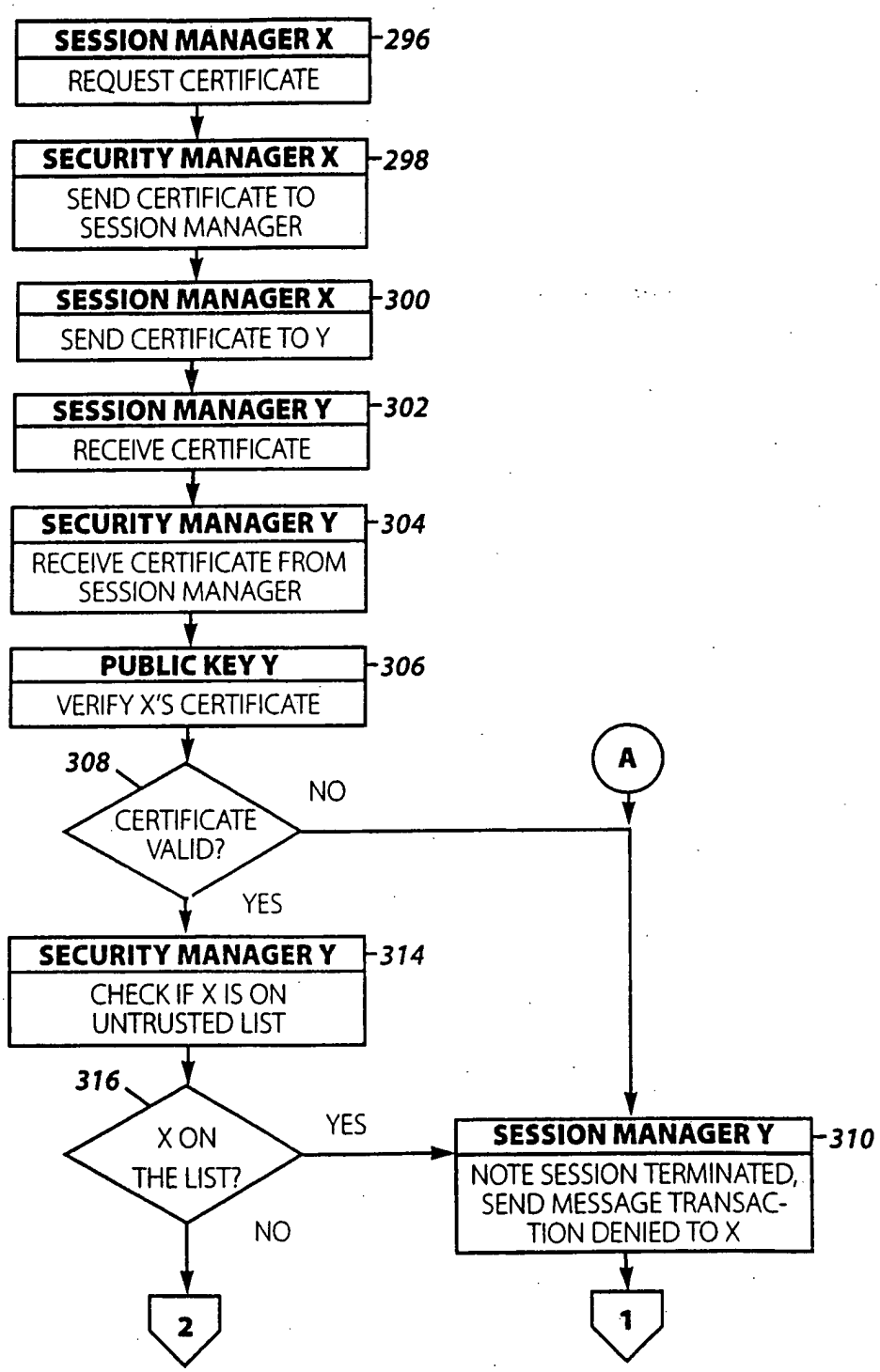
SESSION MANAGER X
REQUEST CERTIFICATE
296
SECURITY MANAGER X
SEND CERTIFICATE TO SESSION MANAGER
298
SESSION MANAGER X
SEND CERTIFICATE TO Y
300
SESSION MANAGER Y
RECEIVE CERTIFICATE
302
SECURITY MANAGER Y
RECEIVE CERTIFICATE FROM SESSION MANAGER
304
PUBLIC KEY Y
VERIFY X'S CERTIFICATE
306
308
CERTIFICATE VALID?
NO
YES
A
SECURITY MANAGER Y
CHECK IF X IS ON UNTRUSTED LIST
314
316
X ON THE LIST?
YES
NO
SESSION MANAGER Y
NOTE SESSION TERMINATED, SEND MESSAGE TRANSAC-TION DENIED TO X
310
2
1

Figure 9A

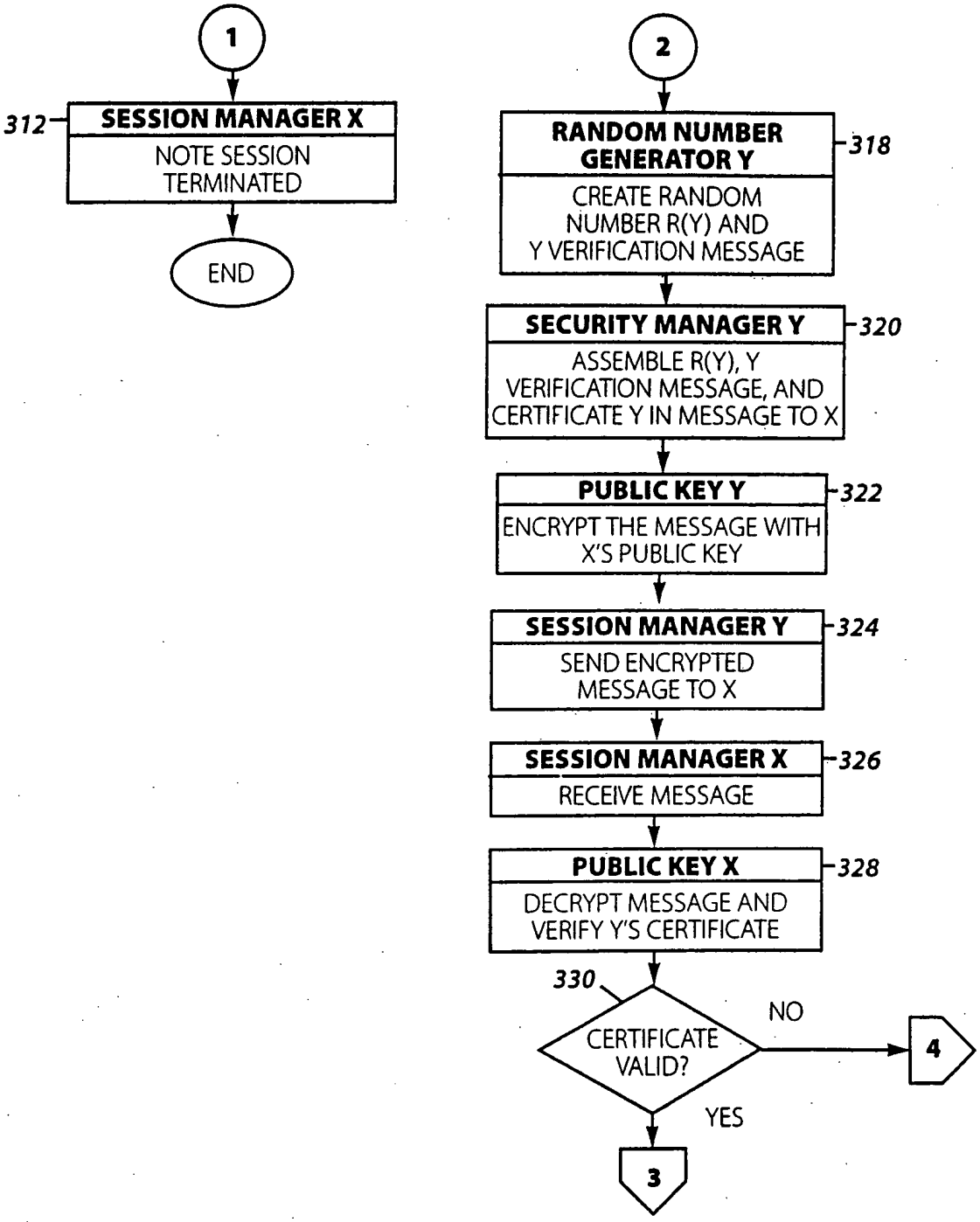
1
312
SESSION MANAGER X
NOTE SESSION TERMINATED
END
2
RANDOM NUMBER GENERATOR Y
318
CREATE RANDOM NUMBER R(Y) AND Y VERIFICATION MESSAGE
SECURITY MANAGER Y
320
ASSEMBLE R(Y), Y VERIFICATION MESSAGE, AND CERTIFICATE Y IN MESSAGE TO X
PUBLIC KEY Y
322
ENCRYPT THE MESSAGE WITH X'S PUBLIC KEY
SESSION MANAGER Y
324
SEND ENCRYPTED MESSAGE TO X
SESSION MANAGER X
326
RECEIVE MESSAGE
PUBLIC KEY X
328
DECRYPT MESSAGE AND VERIFY Y'S CERTIFICATE
330
CERTIFICATE VALID?
NO
4
YES
3

Figure 9B

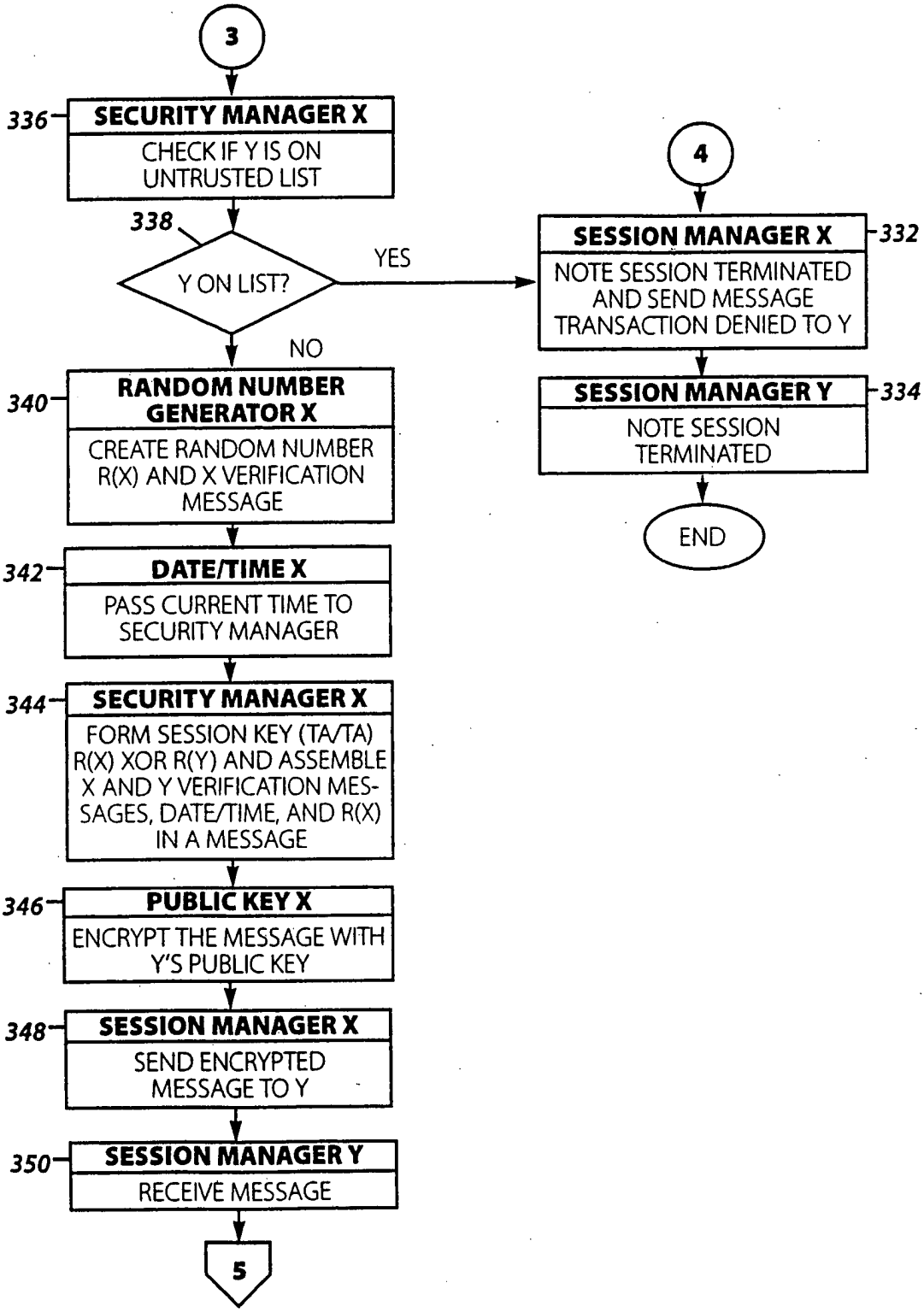
3
336
SECURITY MANAGER X
CHECK IF Y IS ON UNTRUSTED LIST
338
Y ON LIST?
YES
NO
4
SESSION MANAGER X
332
NOTE SESSION TERMINATED AND SEND MESSAGE TRANSACTION DENIED TO Y
SESSION MANAGER Y
334
NOTE SESSION TERMINATED
END
340
RANDOM NUMBER GENERATOR X
CREATE RANDOM NUMBER R(X) AND X VERIFICATION MESSAGE
342
DATE/TIME X
PASS CURRENT TIME TO SECURITY MANAGER
344
SECURITY MANAGER X
FORM SESSION KEY (TA/TA) R(X) XOR R(Y) AND ASSEMBLE X AND Y VERIFICATION MESSAGES, DATE/TIME, AND R(X) IN A MESSAGE
346
PUBLIC KEY X
ENCRYPT THE MESSAGE WITH Y'S PUBLIC KEY
348
SESSION MANAGER X
SEND ENCRYPTED MESSAGE TO Y
350
SESSION MANAGER Y
RECEIVE MESSAGE
5

Figure 9C

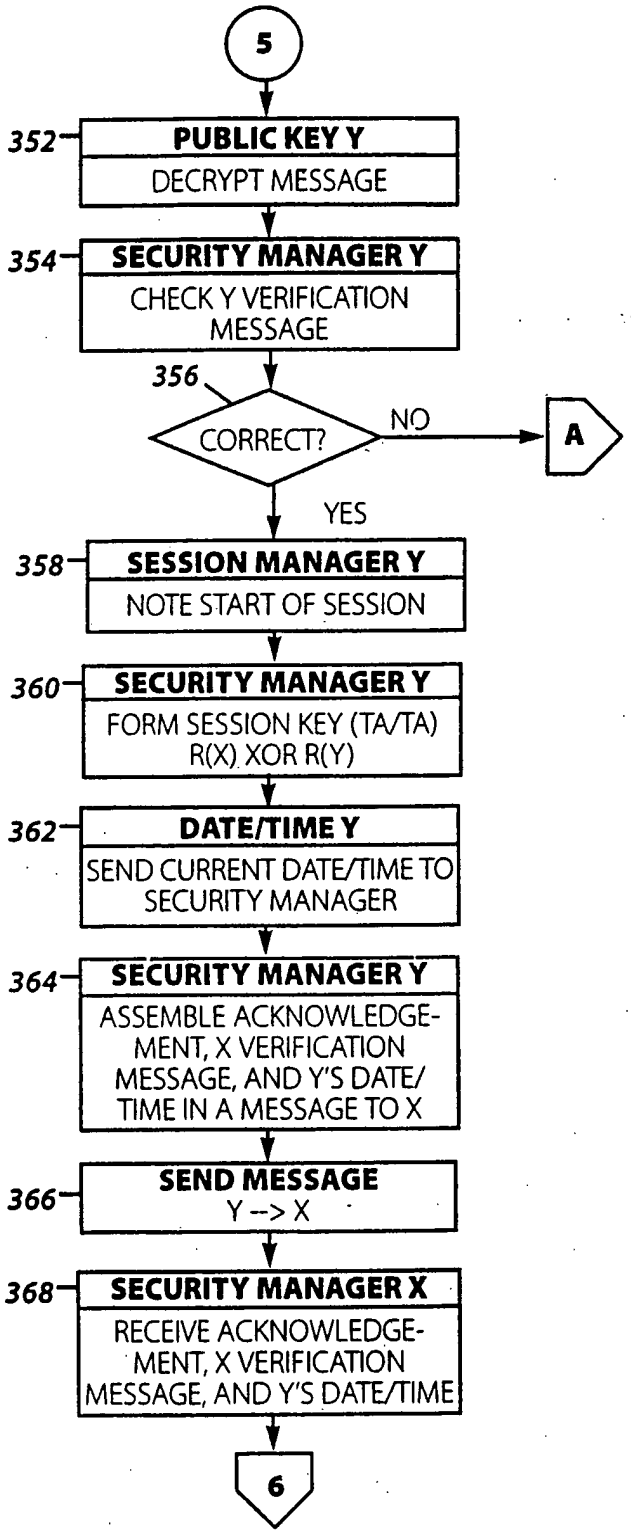
5
352
PUBLIC KEY Y
DECRYPT MESSAGE
354
SECURITY MANAGER Y
CHECK Y VERIFICATION MESSAGE
356
CORRECT?
NO
A
YES
358
SESSION MANAGER Y
NOTE START OF SESSION
360
SECURITY MANAGER Y
FORM SESSION KEY (TA/TA) R(X) XOR R(Y)
362
DATE/TIME Y
SEND CURRENT DATE/TIME TO SECURITY MANAGER
364
SECURITY MANAGER Y
ASSEMBLE ACKNOWLEDGE-MENT, X VERIFICATION MESSAGE, AND Y'S DATE/TIME IN A MESSAGE TO X
366
SEND MESSAGE
Y --> X
368
SECURITY MANAGER X
RECEIVE ACKNOWLEDGE-MENT, X VERIFICATION MESSAGE, AND Y'S DATE/TIME
6

Figure 9D

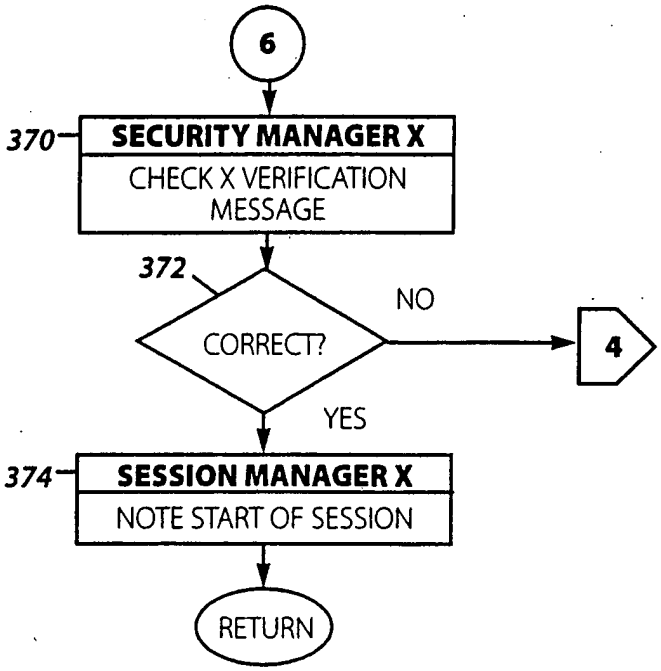
6
370
SECURITY MANAGER X
CHECK X VERIFICATION MESSAGE
372
CORRECT?
NO
4
YES
374
SESSION MANAGER X
NOTE START OF SESSION
RETURN

Figure 9E

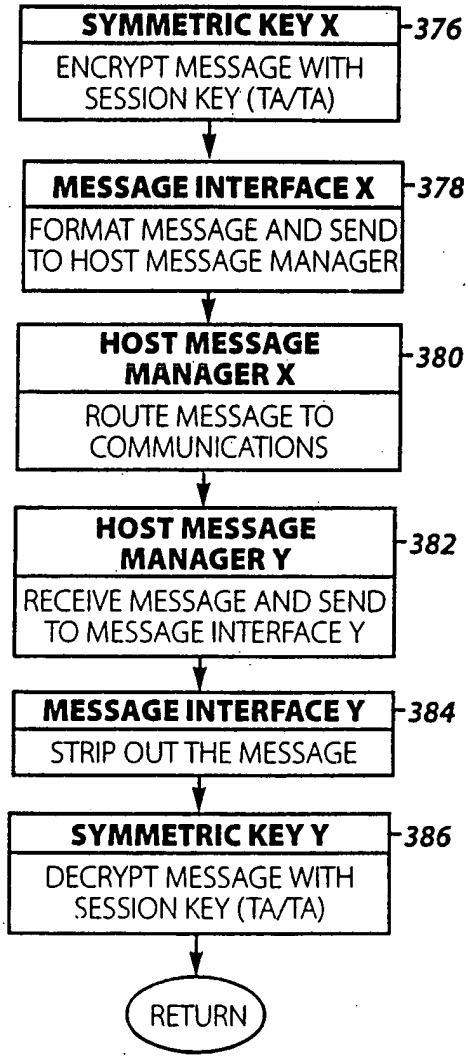
SYMMETRIC KEY X
376
ENCRYPT MESSAGE WITH SESSION KEY (TA/TA)
MESSAGE INTERFACE X
378
FORMAT MESSAGE AND SEND TO HOST MESSAGE MANAGER
HOST MESSAGE MANAGER X
380
ROUTE MESSAGE TO COMMUNICATIONS
HOST MESSAGE MANAGER Y
382
RECEIVE MESSAGE AND SEND TO MESSAGE INTERFACE Y
MESSAGE INTERFACE Y
384
STRIP OUT THE MESSAGE
SYMMETRIC KEY Y
386
DECRYPT MESSAGE WITH SESSION KEY (TA/TA)
RETURN

Figure 10

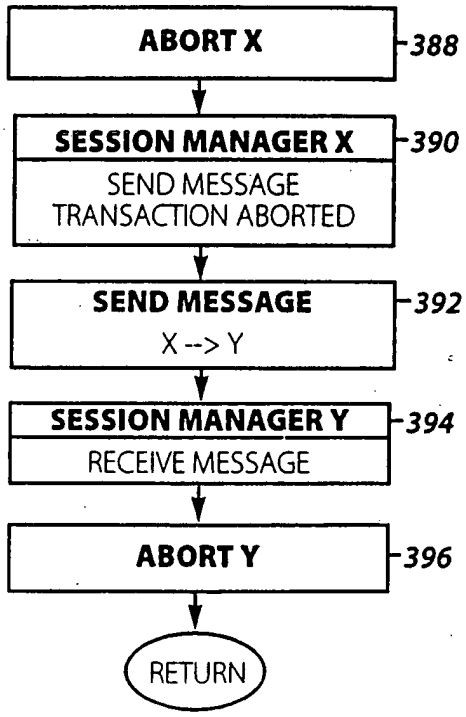
ABORT X
388
SESSION MANAGER X
390
SEND MESSAGE
TRANSACTION ABORTED
SEND MESSAGE
X --> Y
392
SESSION MANAGER Y
394
RECEIVE MESSAGE
ABORT Y
396
RETURN

Figure 11

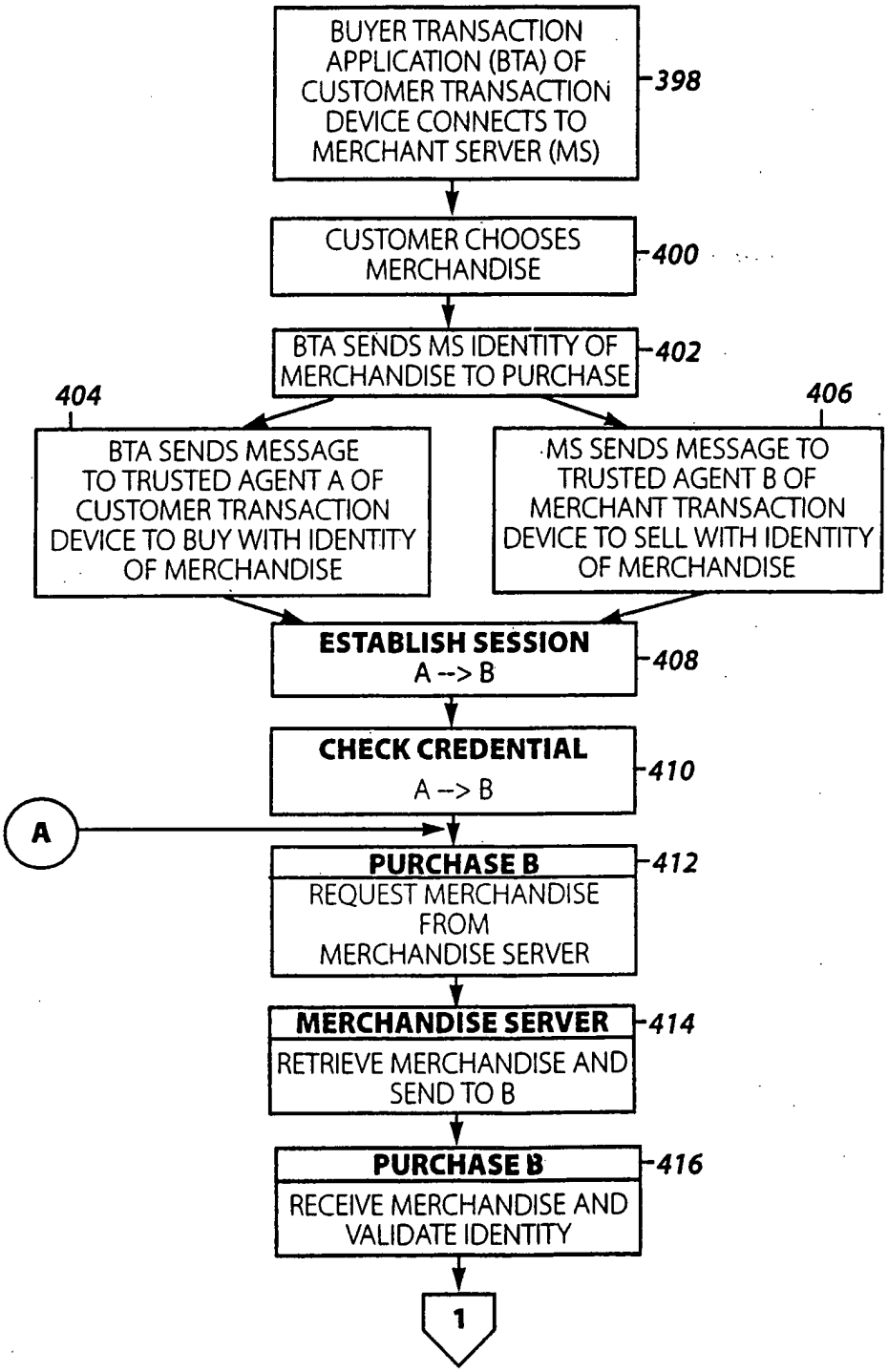
BUYER TRANSACTION APPLICATION (BTA) OF CUSTOMER TRANSACTION DEVICE CONNECTS TO MERCHANT SERVER (MS)
398
CUSTOMER CHOOSES MERCHANDISE
400
BTA SENDS MS IDENTITY OF MERCHANDISE TO PURCHASE
402
404
406
BTA SENDS MESSAGE TO TRUSTED AGENT A OF CUSTOMER TRANSACTION DEVICE TO BUY WITH IDENTITY OF MERCHANDISE
MS SENDS MESSAGE TO TRUSTED AGENT B OF MERCHANT TRANSACTION DEVICE TO SELL WITH IDENTITY OF MERCHANDISE
ESTABLISH SESSION
A --> B
408
CHECK CREDENTIAL
A --> B
410
A
PURCHASE B
REQUEST MERCHANDISE FROM MERCHANDISE SERVER
412
MERCHANDISE SERVER
RETRIEVE MERCHANDISE AND SEND TO B
414
PURCHASE B
RECEIVE MERCHANDISE AND VALIDATE IDENTITY
416
1

Figure 12A

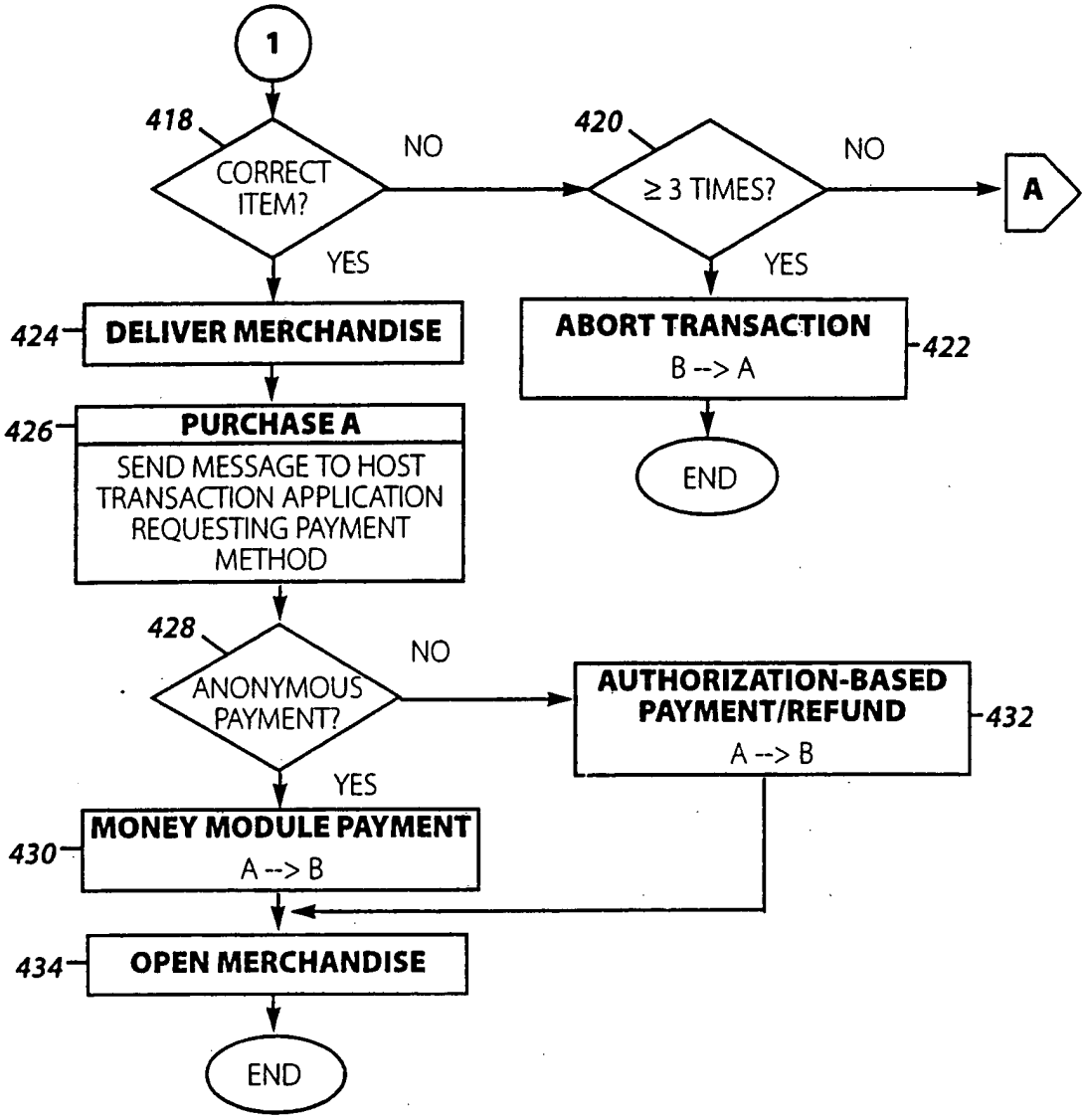
1
418
CORRECT ITEM?
NO
420
≥ 3 TIMES?
NO
A
YES
YES
424
DELIVER MERCHANDISE
ABORT TRANSACTION
B --> A
422
END
426
PURCHASE A
SEND MESSAGE TO HOST TRANSACTION APPLICATION REQUESTING PAYMENT METHOD
428
ANONYMOUS PAYMENT?
NO
AUTHORIZATION-BASED PAYMENT/REFUND
A --> B
432
YES
430
MONEY MODULE PAYMENT
A --> B
434
OPEN MERCHANDISE
END

Figure 12B

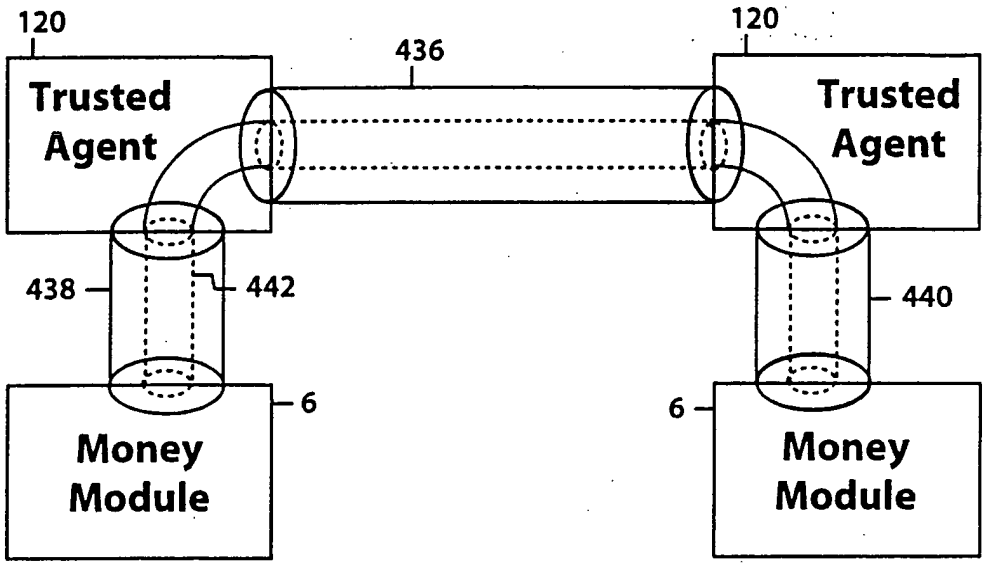
120
436
120
Trusted Agent
Trusted Agent
438
442
440
6
6
Money Module
Money Module

Figure 13

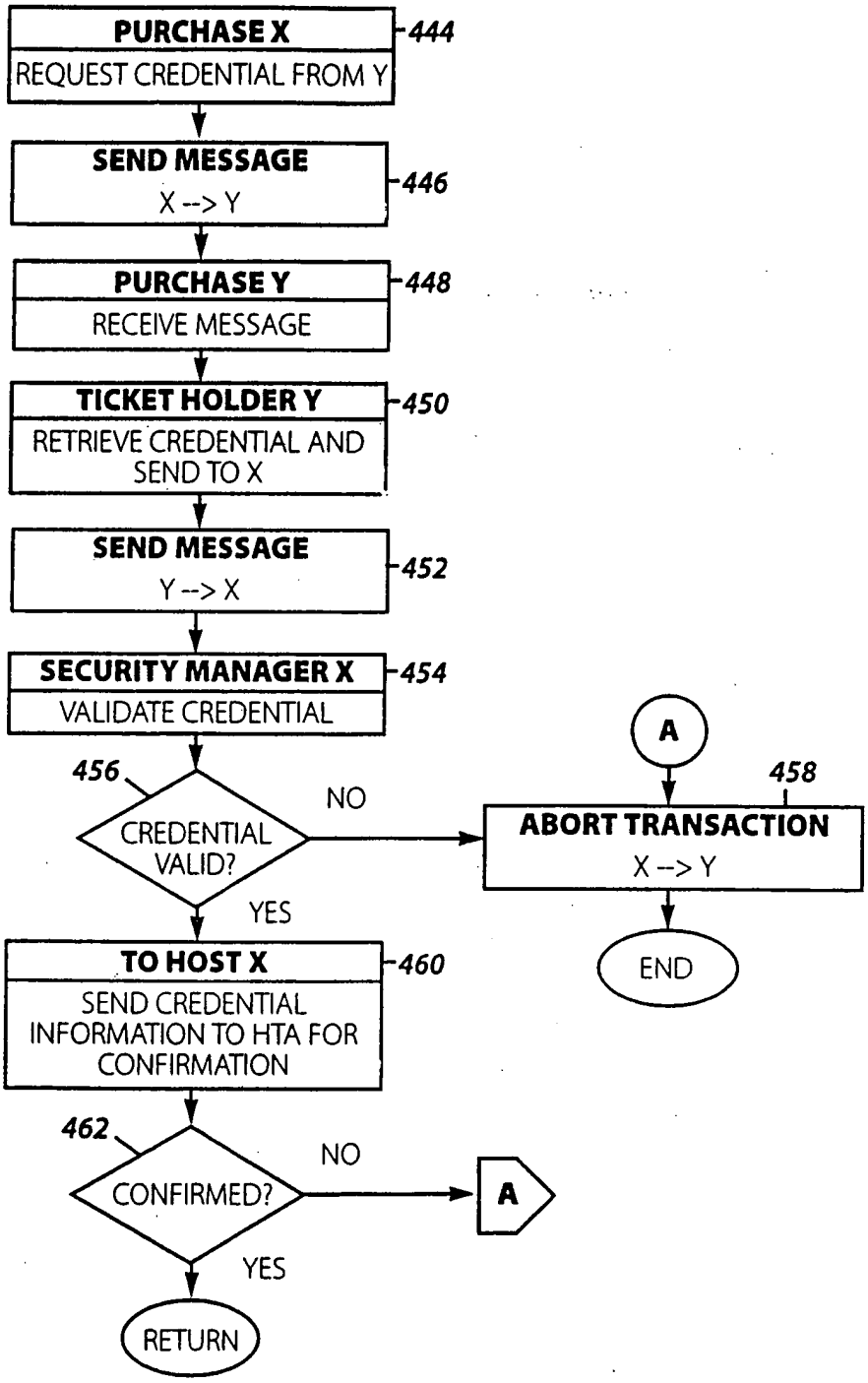
PURCHASE X
REQUEST CREDENTIAL FROM Y
444
SEND MESSAGE
X --> Y
446
PURCHASE Y
RECEIVE MESSAGE
448
TICKET HOLDER Y
RETRIEVE CREDENTIAL AND SEND TO X
450
SEND MESSAGE
Y --> X
452
SECURITY MANAGER X
VALIDATE CREDENTIAL
454
456
CREDENTIAL VALID?
NO
YES
A
458
ABORT TRANSACTION
X --> Y
END
TO HOST X
SEND CREDENTIAL INFORMATION TO HTA FOR CONFIRMATION
460
462
CONFIRMED?
NO
A
YES
RETURN

Figure 14

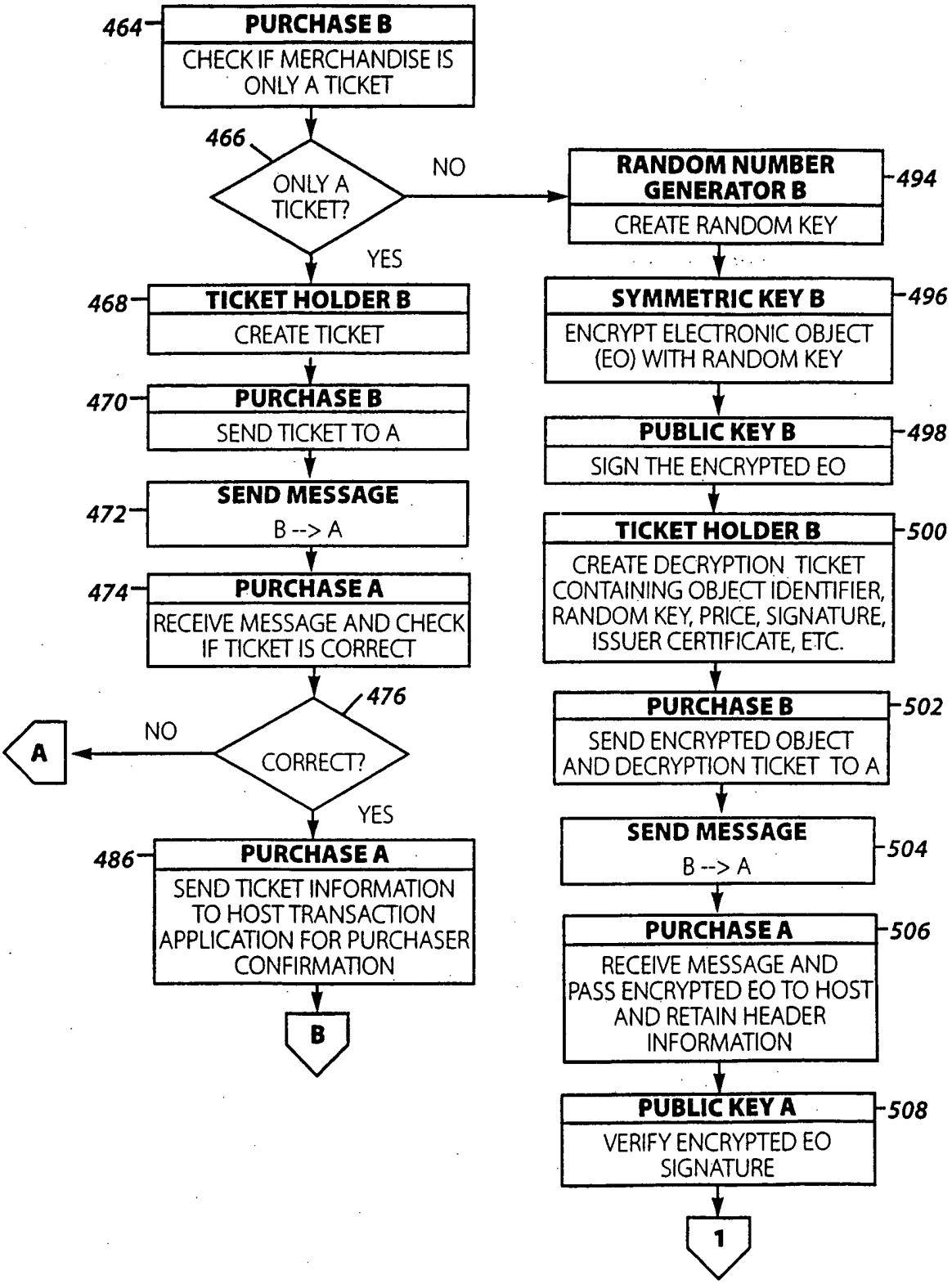
464
PURCHASE B
CHECK IF MERCHANDISE IS ONLY A TICKET
466
ONLY A TICKET?
NO
YES
RANDOM NUMBER GENERATOR B
494
CREATE RANDOM KEY
468
TICKET HOLDER B
CREATE TICKET
SYMMETRIC KEY B
496
ENCRYPT ELECTRONIC OBJECT (EO) WITH RANDOM KEY
470
PURCHASE B
SEND TICKET TO A
PUBLIC KEY B
498
SIGN THE ENCRYPTED EO
472
SEND MESSAGE
B --> A
TICKET HOLDER B
500
CREATE DECRYPTION TICKET CONTAINING OBJECT IDENTIFIER, RANDOM KEY, PRICE, SIGNATURE, ISSUER CERTIFICATE, ETC.
474
PURCHASE A
RECEIVE MESSAGE AND CHECK IF TICKET IS CORRECT
476
A
NO
CORRECT?
YES
PURCHASE B
502
SEND ENCRYPTED OBJECT AND DECRYPTION TICKET TO A
SEND MESSAGE
504
B --> A
PURCHASE A
506
RECEIVE MESSAGE AND PASS ENCRYPTED EO TO HOST AND RETAIN HEADER INFORMATION
486
PURCHASE A
SEND TICKET INFORMATION TO HOST TRANSACTION APPLICATION FOR PURCHASER CONFIRMATION
PUBLIC KEY A
508
VERIFY ENCRYPTED EO SIGNATURE
B
1

Figure 15A

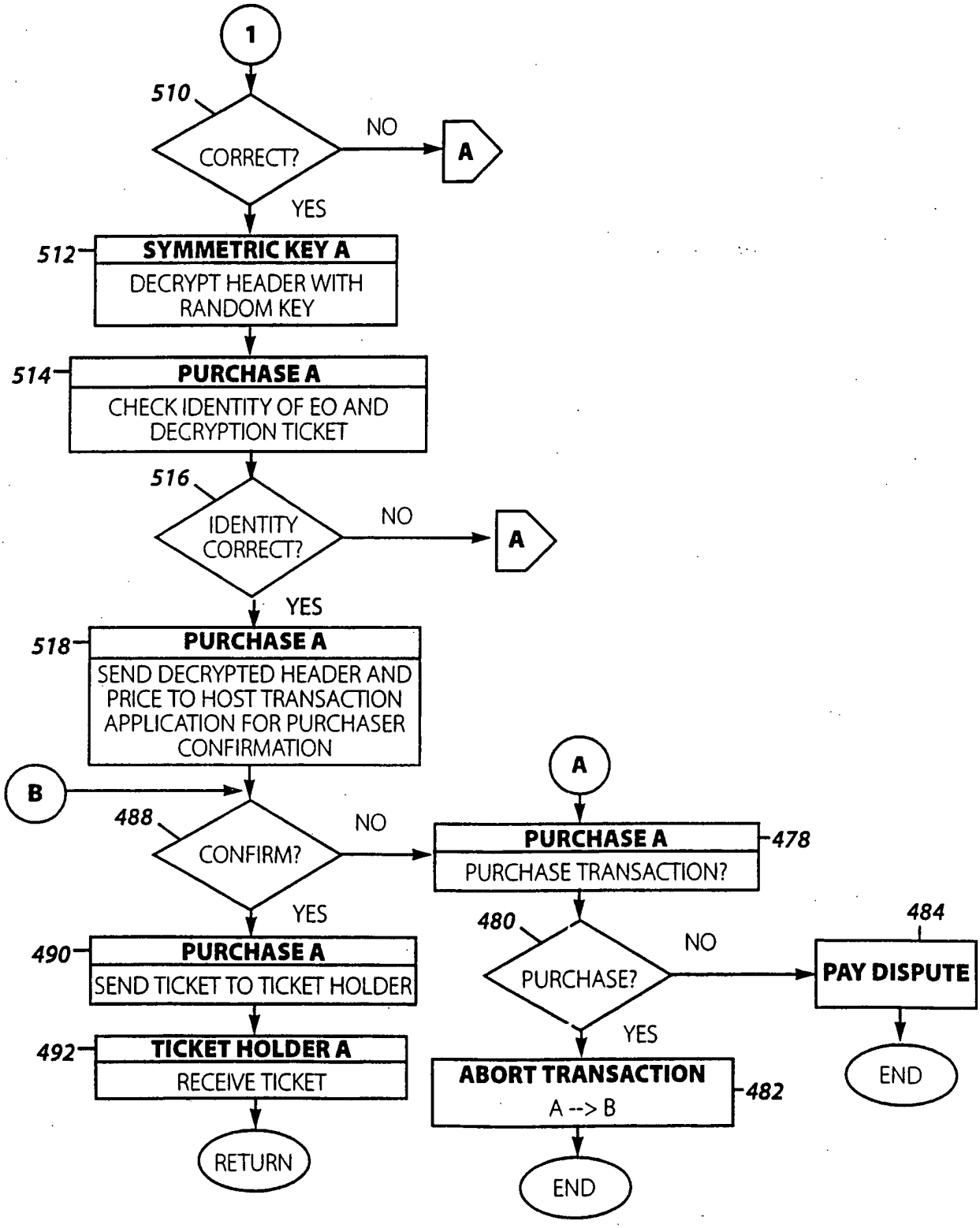
1
510
CORRECT?
NO
A
YES
512
SYMMETRIC KEY A
DECRYPT HEADER WITH RANDOM KEY
514
PURCHASE A
CHECK IDENTITY OF EO AND DECRYPTION TICKET
516
IDENTITY CORRECT?
NO
A
YES
518
PURCHASE A
SEND DECRYPTED HEADER AND PRICE TO HOST TRANSACTION APPLICATION FOR PURCHASER CONFIRMATION
B
488
CONFIRM?
NO
YES
A
PURCHASE A
478
PURCHASE TRANSACTION?
480
PURCHASE?
NO
484
PAY DISPUTE
END
YES
490
PURCHASE A
SEND TICKET TO TICKET HOLDER
492
TICKET HOLDER A
RECEIVE TICKET
RETURN
ABORT TRANSACTION
A --> B
482
END

Figure 15B

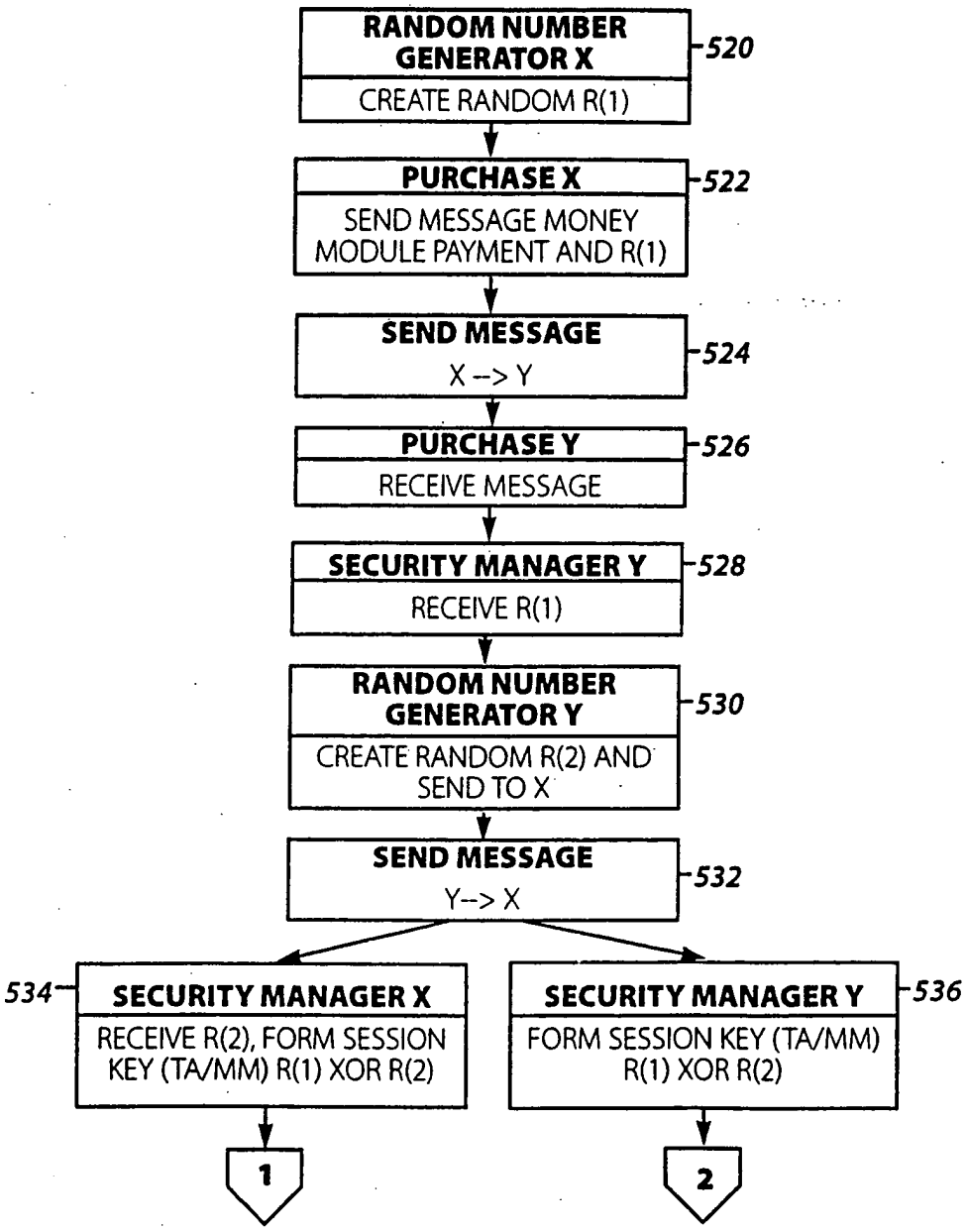
RANDOM NUMBER GENERATOR X
CREATE RANDOM R(1)
520
PURCHASE X
SEND MESSAGE MONEY MODULE PAYMENT AND R(1)
522
SEND MESSAGE
X --> Y
524
PURCHASE Y
RECEIVE MESSAGE
526
SECURITY MANAGER Y
RECEIVE R(1)
528
RANDOM NUMBER GENERATOR Y
CREATE RANDOM R(2) AND SEND TO X
530
SEND MESSAGE
Y--> X
532
534
SECURITY MANAGER X
RECEIVE R(2), FORM SESSION KEY (TA/MM) R(1) XOR R(2)
SECURITY MANAGER Y
FORM SESSION KEY (TA/MM) R(1) XOR R(2)
536
1
2

Figure 16A

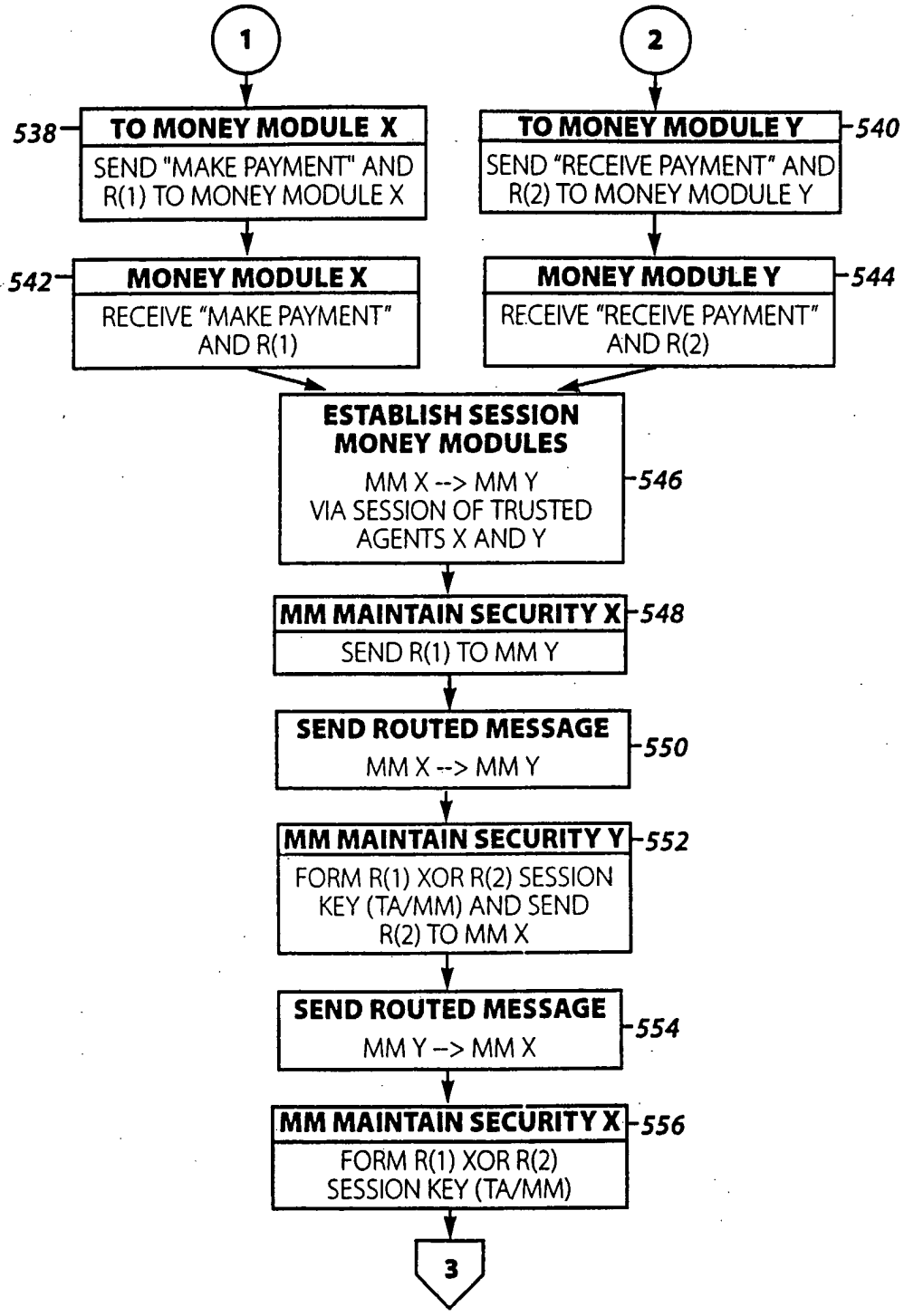
1
2
538
TO MONEY MODULE X
SEND "MAKE PAYMENT" AND R(1) TO MONEY MODULE X
TO MONEY MODULE Y
SEND "RECEIVE PAYMENT" AND R(2) TO MONEY MODULE Y
540
542
MONEY MODULE X
RECEIVE "MAKE PAYMENT" AND R(1)
MONEY MODULE Y
RECEIVE "RECEIVE PAYMENT" AND R(2)
544
ESTABLISH SESSION MONEY MODULES
MM X --> MM Y VIA SESSION OF TRUSTED AGENTS X AND Y
546
MM MAINTAIN SECURITY X
SEND R(1) TO MM Y
548
SEND ROUTED MESSAGE
MM X --> MM Y
550
MM MAINTAIN SECURITY Y
FORM R(1) XOR R(2) SESSION KEY (TA/MM) AND SEND R(2) TO MM X
552
SEND ROUTED MESSAGE
MM Y --> MM X
554
MM MAINTAIN SECURITY X
FORM R(1) XOR R(2) SESSION KEY (TA/MM)
556
3

Figure 16B

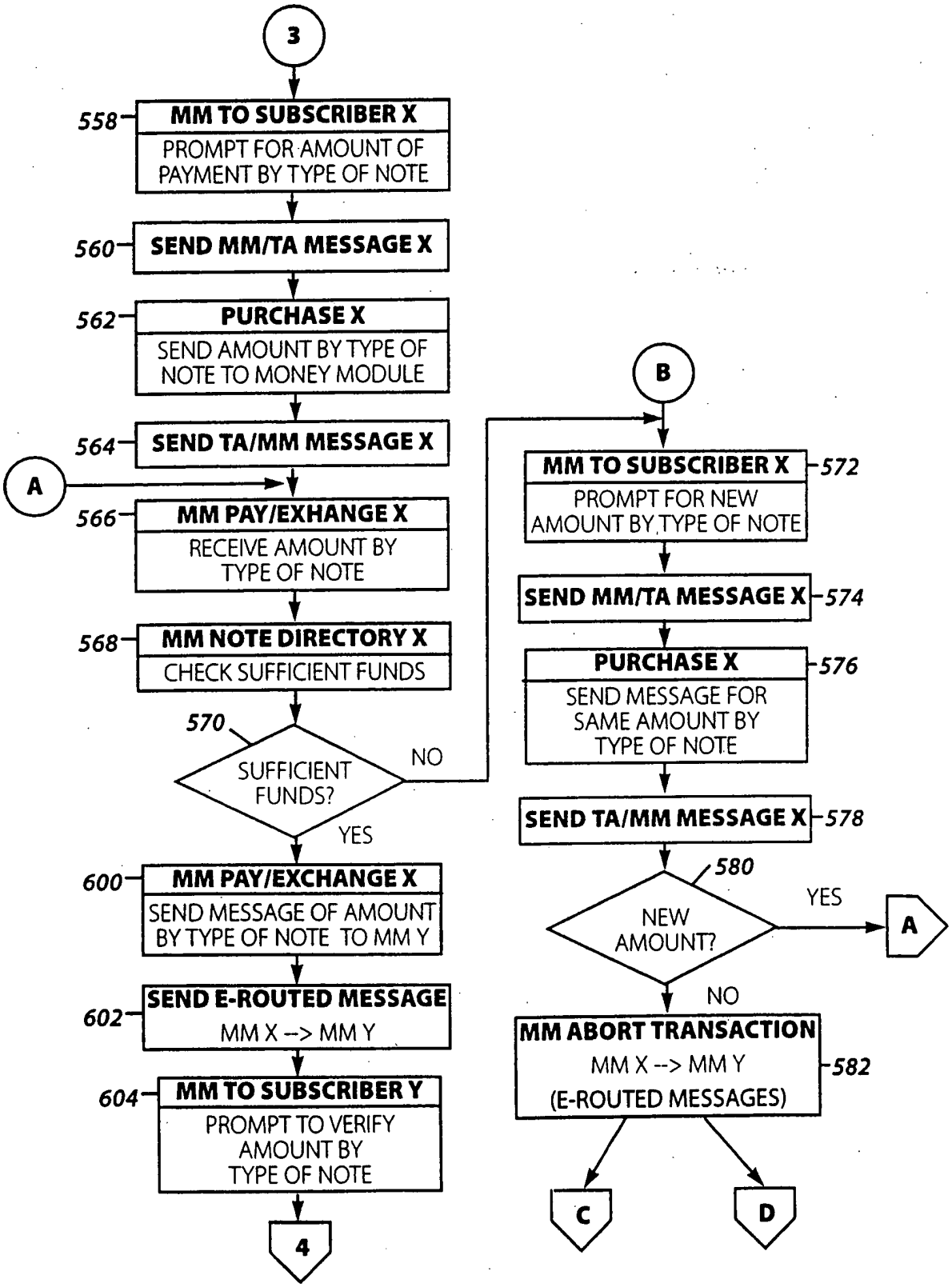
3
558
MM TO SUBSCRIBER X
PROMPT FOR AMOUNT OF PAYMENT BY TYPE OF NOTE
560
SEND MM/TA MESSAGE X
562
PURCHASE X
SEND AMOUNT BY TYPE OF NOTE TO MONEY MODULE
564
SEND TA/MM MESSAGE X
A
566
MM PAY/EXHANGE X
RECEIVE AMOUNT BY TYPE OF NOTE
568
MM NOTE DIRECTORY X
CHECK SUFFICIENT FUNDS
570
SUFFICIENT FUNDS?
NO
YES
600
MM PAY/EXCHANGE X
SEND MESSAGE OF AMOUNT BY TYPE OF NOTE TO MM Y
602
SEND E-ROUTED MESSAGE
MM X --> MM Y
604
MM TO SUBSCRIBER Y
PROMPT TO VERIFY AMOUNT BY TYPE OF NOTE
4
B
572
MM TO SUBSCRIBER X
PROMPT FOR NEW AMOUNT BY TYPE OF NOTE
574
SEND MM/TA MESSAGE X
576
PURCHASE X
SEND MESSAGE FOR SAME AMOUNT BY TYPE OF NOTE
578
SEND TA/MM MESSAGE X
580
NEW AMOUNT?
YES
A
NO
582
MM ABORT TRANSACTION
MM X --> MM Y
(E-ROUTED MESSAGES)
C
D

Figure 16C

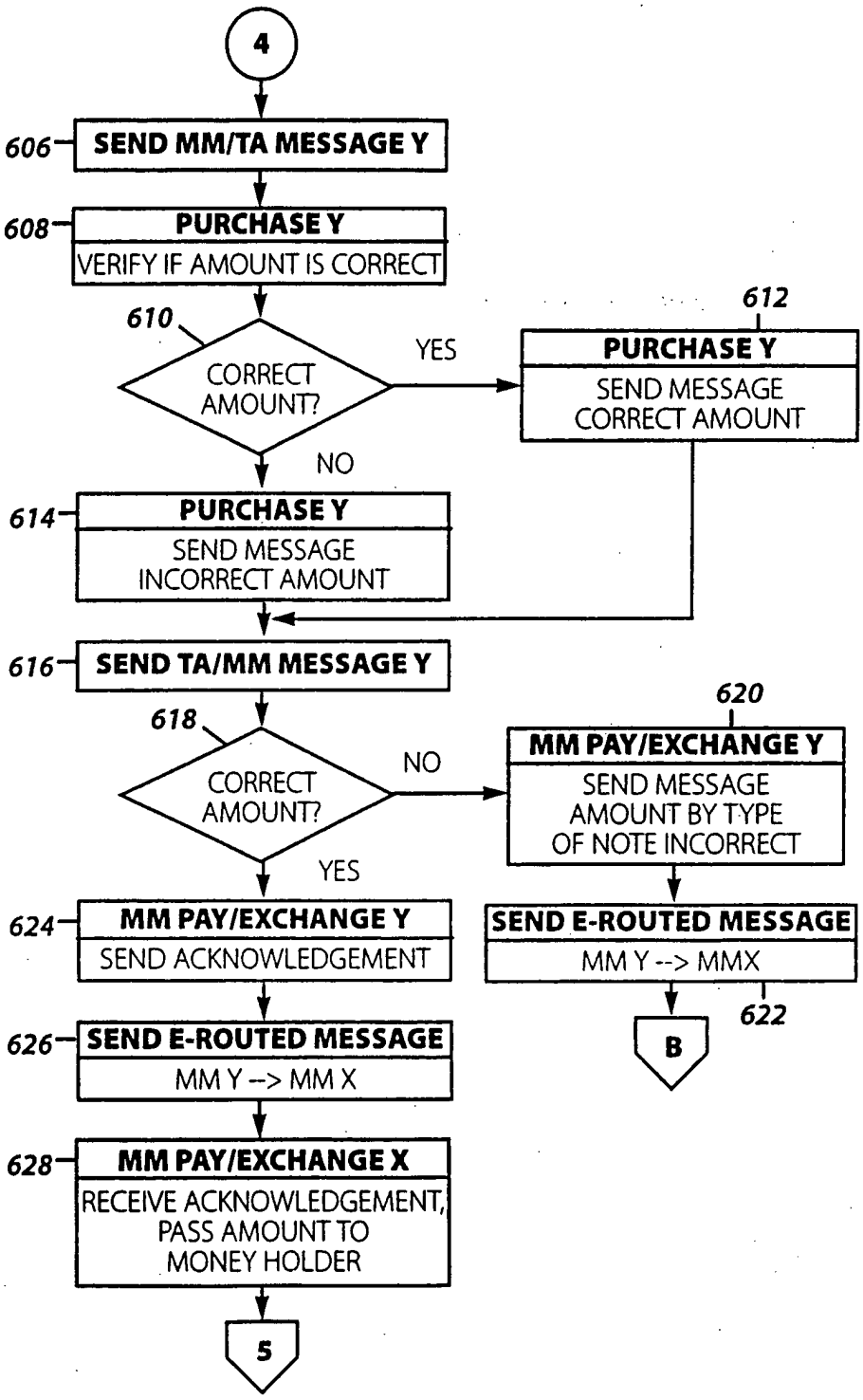
4
606
SEND MM/TA MESSAGE Y
608
PURCHASE Y
VERIFY IF AMOUNT IS CORRECT
610
CORRECT AMOUNT?
YES
612
PURCHASE Y
SEND MESSAGE CORRECT AMOUNT
NO
614
PURCHASE Y
SEND MESSAGE INCORRECT AMOUNT
616
SEND TA/MM MESSAGE Y
618
CORRECT AMOUNT?
NO
620
MM PAY/EXCHANGE Y
SEND MESSAGE AMOUNT BY TYPE OF NOTE INCORRECT
YES
624
MM PAY/EXCHANGE Y
SEND ACKNOWLEDGEMENT
SEND E-ROUTED MESSAGE
MM Y --> MMX
622
B
626
SEND E-ROUTED MESSAGE
MM Y --> MM X
628
MM PAY/EXCHANGE X
RECEIVE ACKNOWLEDGEMENT, PASS AMOUNT TO MONEY HOLDER
5

Figure 16D

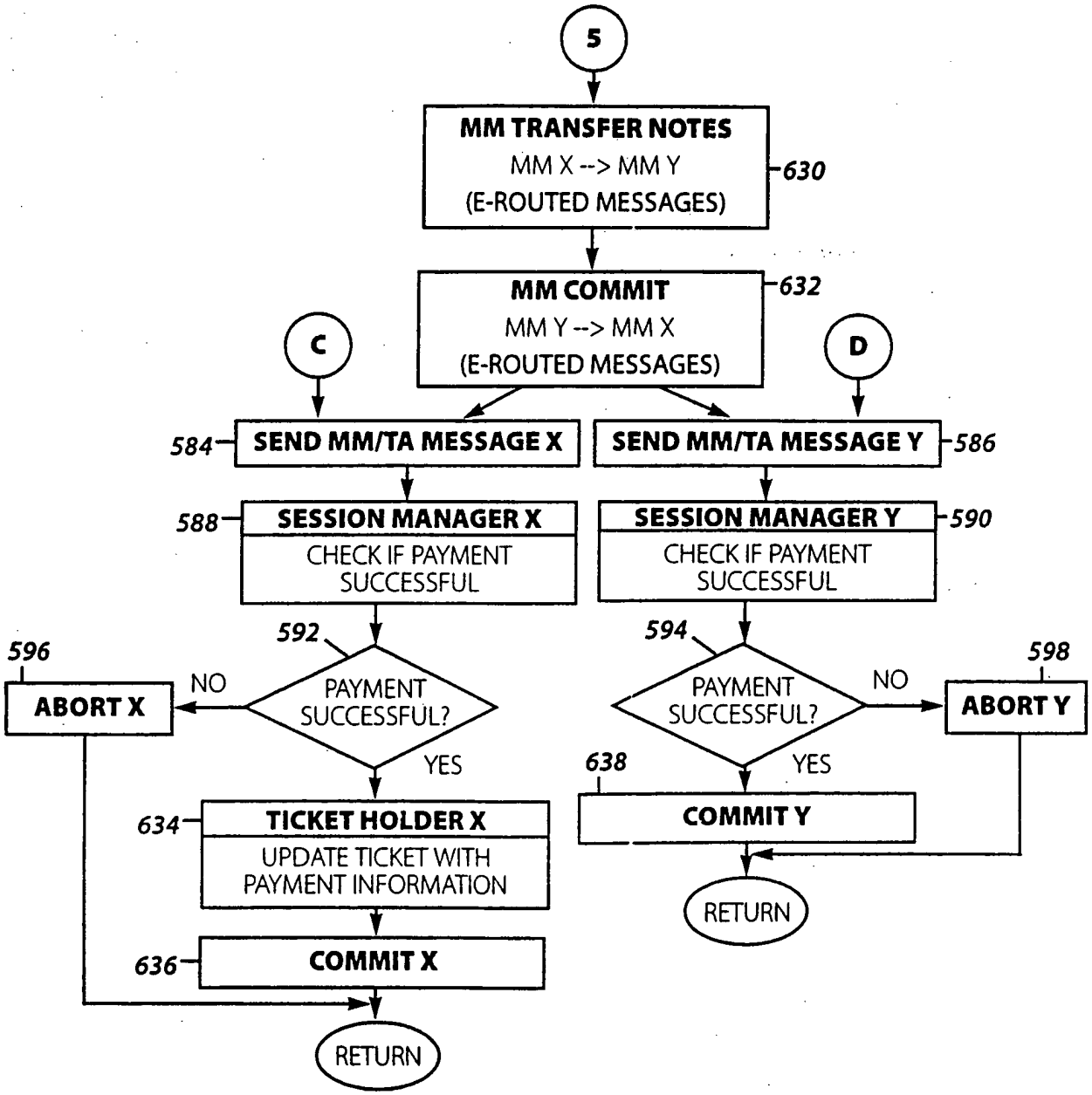
5
MM TRANSFER NOTES
MM X --> MM Y
(E-ROUTED MESSAGES)
630
MM COMMIT
MM Y --> MM X
(E-ROUTED MESSAGES)
632
C
D
584
SEND MM/TA MESSAGE X
SEND MM/TA MESSAGE Y
586
588
SESSION MANAGER X
CHECK IF PAYMENT SUCCESSFUL
SESSION MANAGER Y
CHECK IF PAYMENT SUCCESSFUL
590
592
594
596
ABORT X
NO
PAYMENT SUCCESSFUL?
YES
NO
PAYMENT SUCCESSFUL?
598
ABORT Y
638
YES
634
TICKET HOLDER X
UPDATE TICKET WITH PAYMENT INFORMATION
COMMIT Y
636
COMMIT X
RETURN
RETURN

Figure 16E

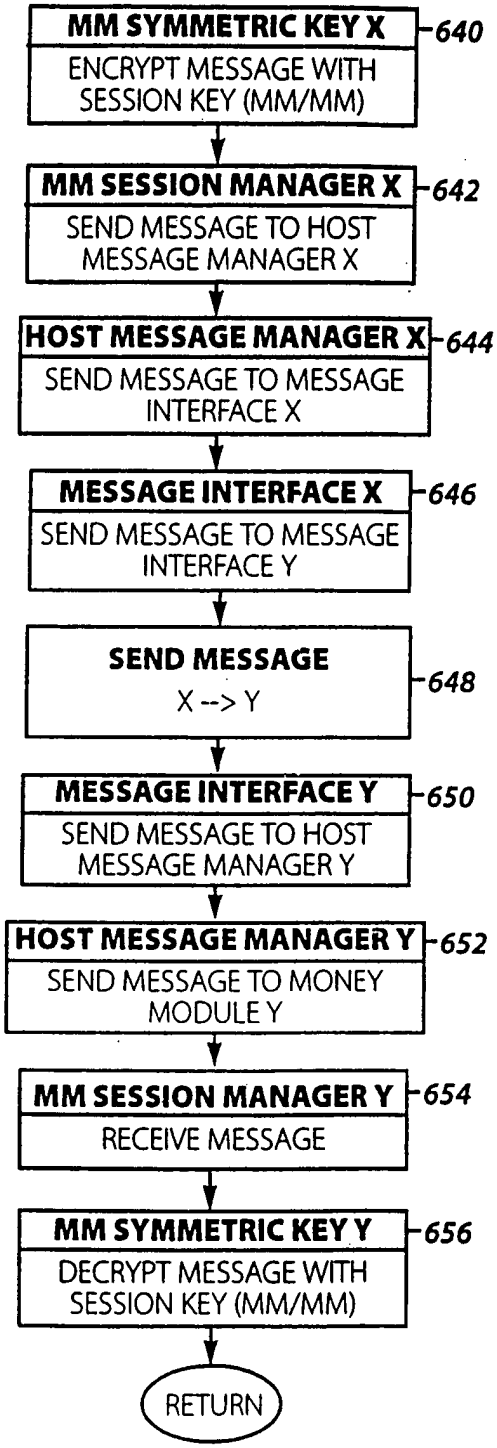
MM SYMMETRIC KEY X
ENCRYPT MESSAGE WITH SESSION KEY (MM/MM)
640
MM SESSION MANAGER X
SEND MESSAGE TO HOST MESSAGE MANAGER X
642
HOST MESSAGE MANAGER X
SEND MESSAGE TO MESSAGE INTERFACE X
644
MESSAGE INTERFACE X
SEND MESSAGE TO MESSAGE INTERFACE Y
646
SEND MESSAGE
X --> Y
648
MESSAGE INTERFACE Y
SEND MESSAGE TO HOST MESSAGE MANAGER Y
650
HOST MESSAGE MANAGER Y
SEND MESSAGE TO MONEY MODULE Y
652
MM SESSION MANAGER Y
RECEIVE MESSAGE
654
MM SYMMETRIC KEY Y
DECRYPT MESSAGE WITH SESSION KEY (MM/MM)
656
RETURN

Figure 17

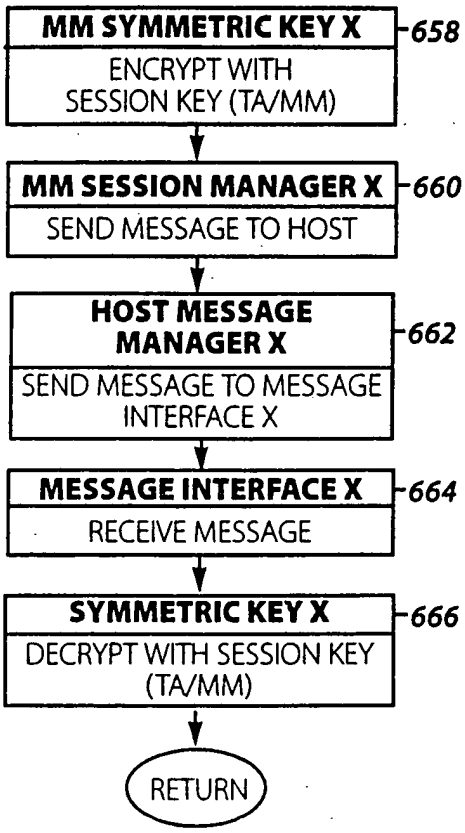
MM SYMMETRIC KEY X
ENCRYPT WITH SESSION KEY (TA/MM)
658
MM SESSION MANAGER X
SEND MESSAGE TO HOST
660
HOST MESSAGE MANAGER X
SEND MESSAGE TO MESSAGE INTERFACE X
662
MESSAGE INTERFACE X
RECEIVE MESSAGE
664
SYMMETRIC KEY X
DECRYPT WITH SESSION KEY (TA/MM)
666
RETURN

Figure 18

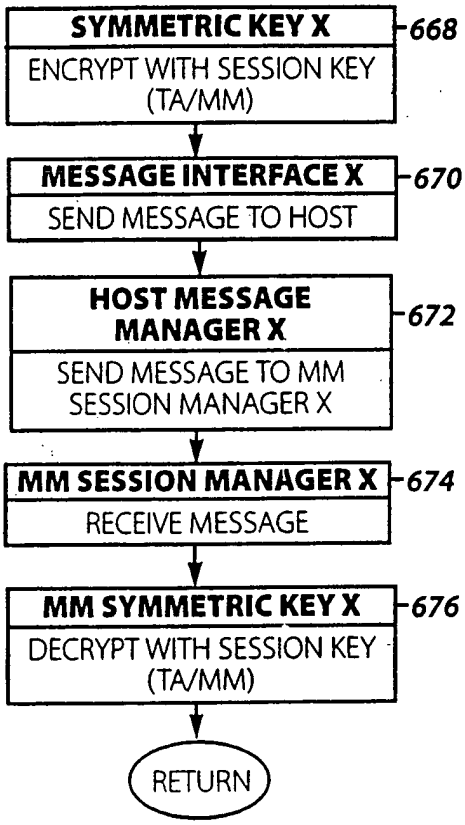
SYMMETRIC KEY X
668
ENCRYPT WITH SESSION KEY (TA/MM)
MESSAGE INTERFACE X
670
SEND MESSAGE TO HOST
HOST MESSAGE MANAGER X
672
SEND MESSAGE TO MM SESSION MANAGER X
MM SESSION MANAGER X
674
RECEIVE MESSAGE
MM SYMMETRIC KEY X
676
DECRYPT WITH SESSION KEY (TA/MM)
RETURN

Figure 19

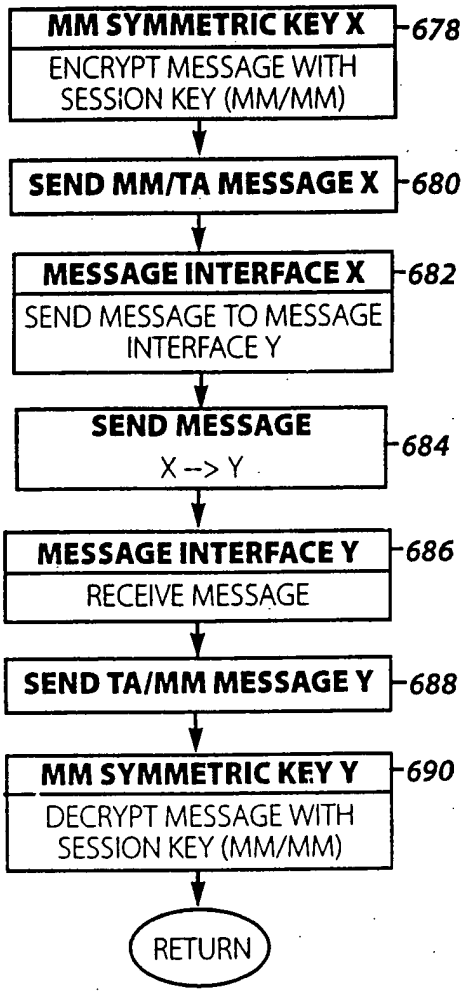
MM SYMMETRIC KEY X
678
ENCRYPT MESSAGE WITH SESSION KEY (MM/MM)
SEND MM/TA MESSAGE X
680
MESSAGE INTERFACE X
682
SEND MESSAGE TO MESSAGE INTERFACE Y
SEND MESSAGE
X --> Y
684
MESSAGE INTERFACE Y
686
RECEIVE MESSAGE
SEND TA/MM MESSAGE Y
688
MM SYMMETRIC KEY Y
690
DECRYPT MESSAGE WITH SESSION KEY (MM/MM)
RETURN

Figure 20

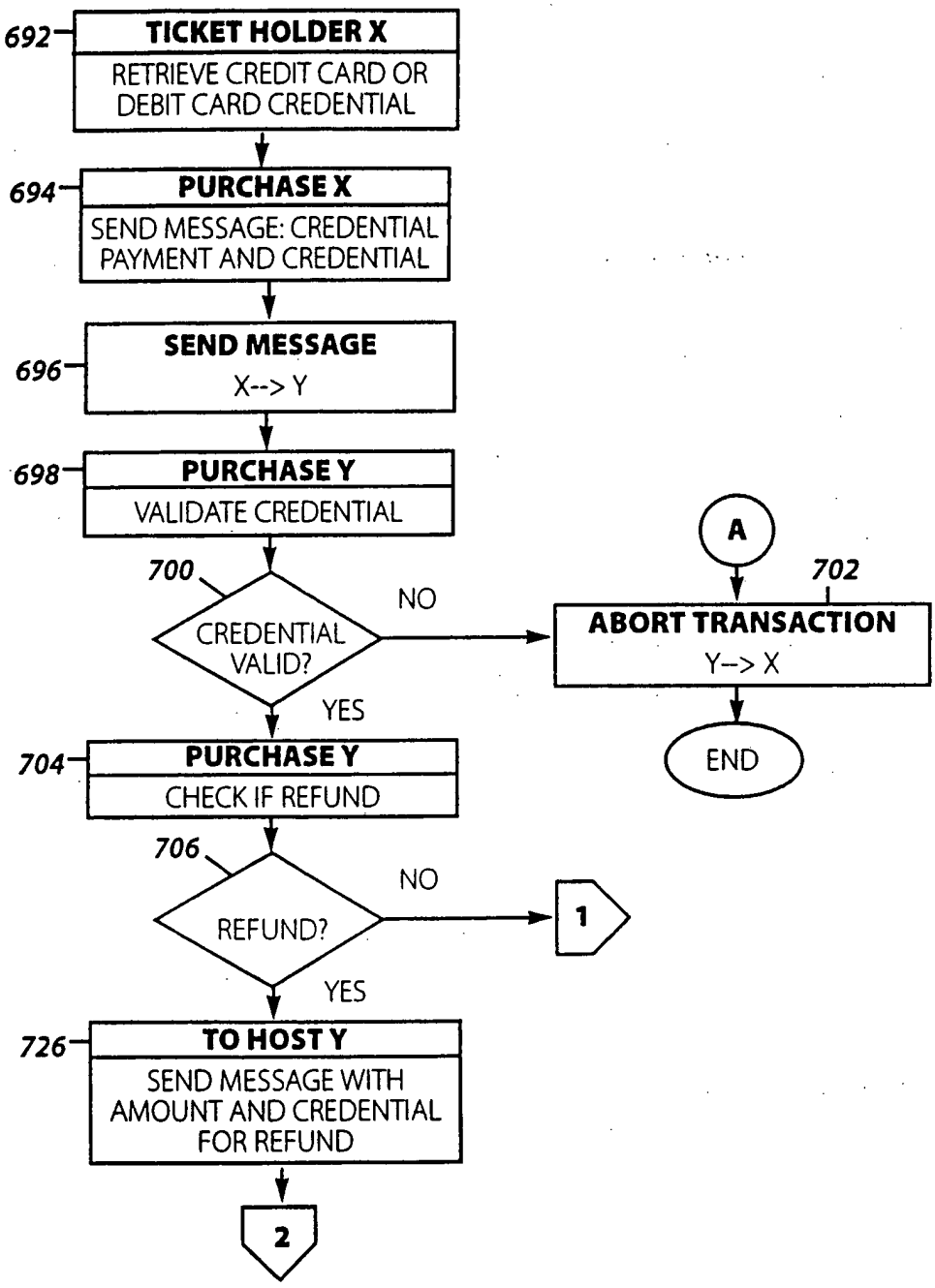
692
TICKET HOLDER X
RETRIEVE CREDIT CARD OR DEBIT CARD CREDENTIAL
694
PURCHASE X
SEND MESSAGE: CREDENTIAL PAYMENT AND CREDENTIAL
696
SEND MESSAGE
X--> Y
698
PURCHASE Y
VALIDATE CREDENTIAL
700
CREDENTIAL VALID?
NO
YES
A
702
ABORT TRANSACTION
Y--> X
END
704
PURCHASE Y
CHECK IF REFUND
706
REFUND?
NO
1
YES
726
TO HOST Y
SEND MESSAGE WITH AMOUNT AND CREDENTIAL FOR REFUND
2

Figure 21A

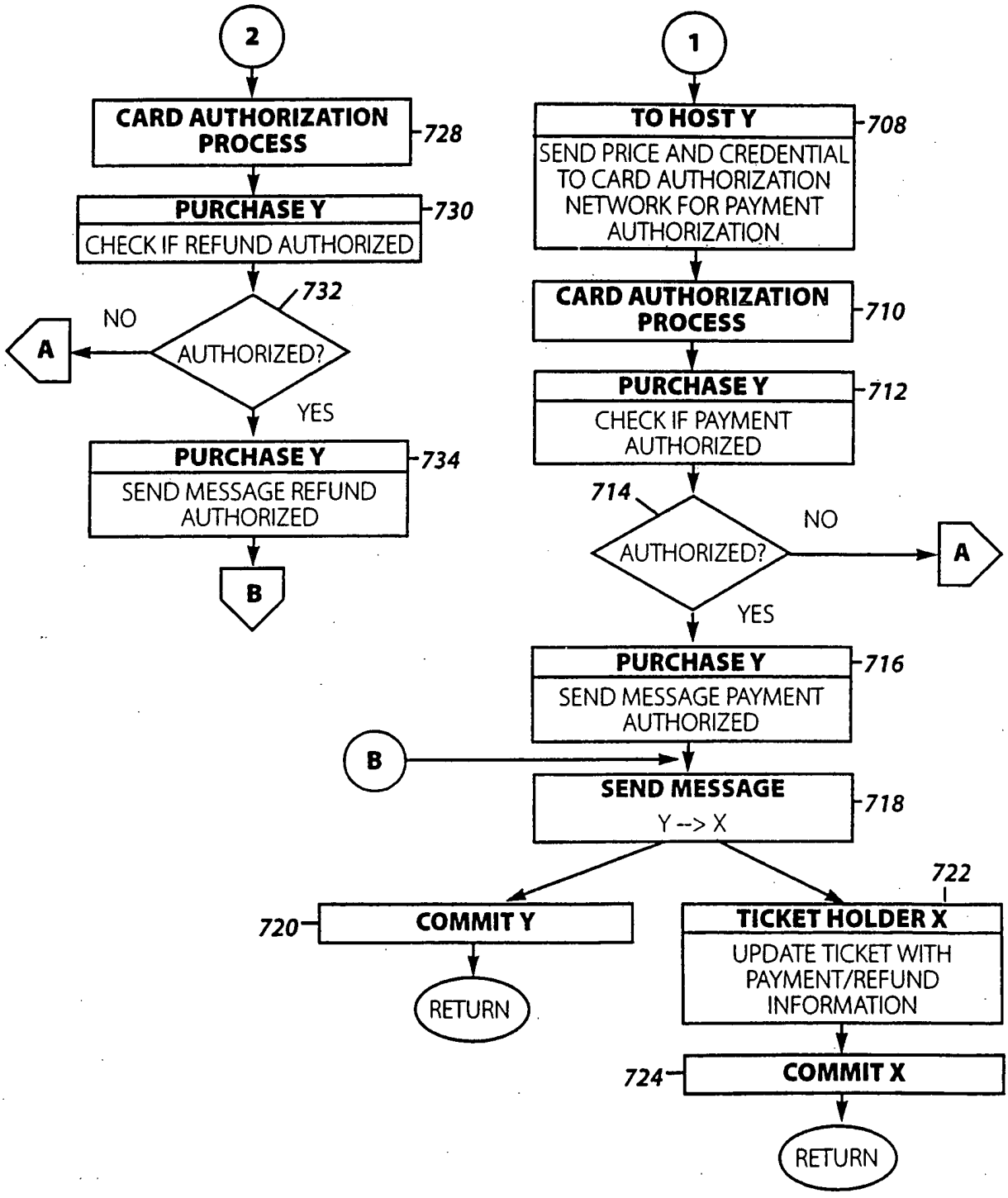
2
CARD AUTHORIZATION PROCESS
728
PURCHASE Y
CHECK IF REFUND AUTHORIZED
730
732
NO
A
AUTHORIZED?
YES
PURCHASE Y
SEND MESSAGE REFUND AUTHORIZED
734
B
1
TO HOST Y
SEND PRICE AND CREDENTIAL TO CARD AUTHORIZATION NETWORK FOR PAYMENT AUTHORIZATION
708
CARD AUTHORIZATION PROCESS
710
PURCHASE Y
CHECK IF PAYMENT AUTHORIZED
712
714
NO
AUTHORIZED?
A
YES
PURCHASE Y
SEND MESSAGE PAYMENT AUTHORIZED
716
B
SEND MESSAGE
Y --> X
718
722
720
COMMIT Y
RETURN
TICKET HOLDER X
UPDATE TICKET WITH PAYMENT/REFUND INFORMATION
724
COMMIT X
RETURN

Figure 21B

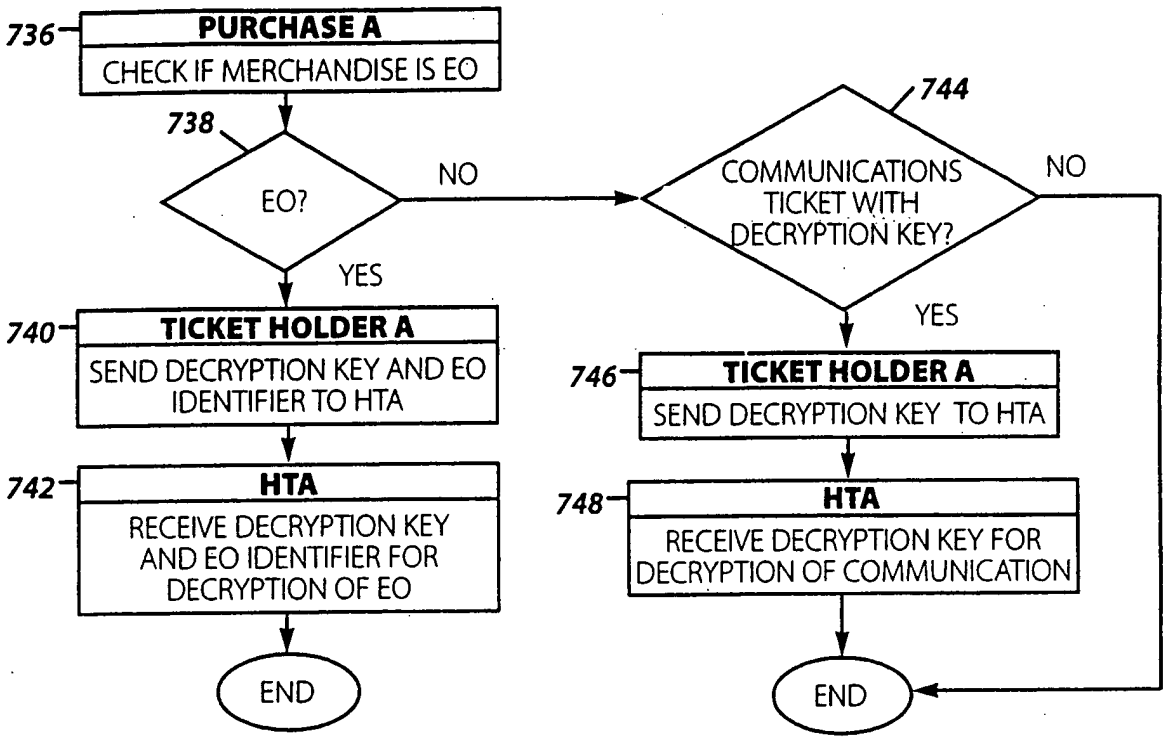
736
PURCHASE A
CHECK IF MERCHANDISE IS EO
738
EO?
NO
YES
740
TICKET HOLDER A
SEND DECRYPTION KEY AND EO IDENTIFIER TO HTA
742
HTA
RECEIVE DECRYPTION KEY AND EO IDENTIFIER FOR DECRYPTION OF EO
END
744
COMMUNICATIONS TICKET WITH DECRYPTION KEY?
NO
YES
746
TICKET HOLDER A
SEND DECRYPTION KEY TO HTA
748
HTA
RECEIVE DECRYPTION KEY FOR DECRYPTION OF COMMUNICATION
END

Figure 22

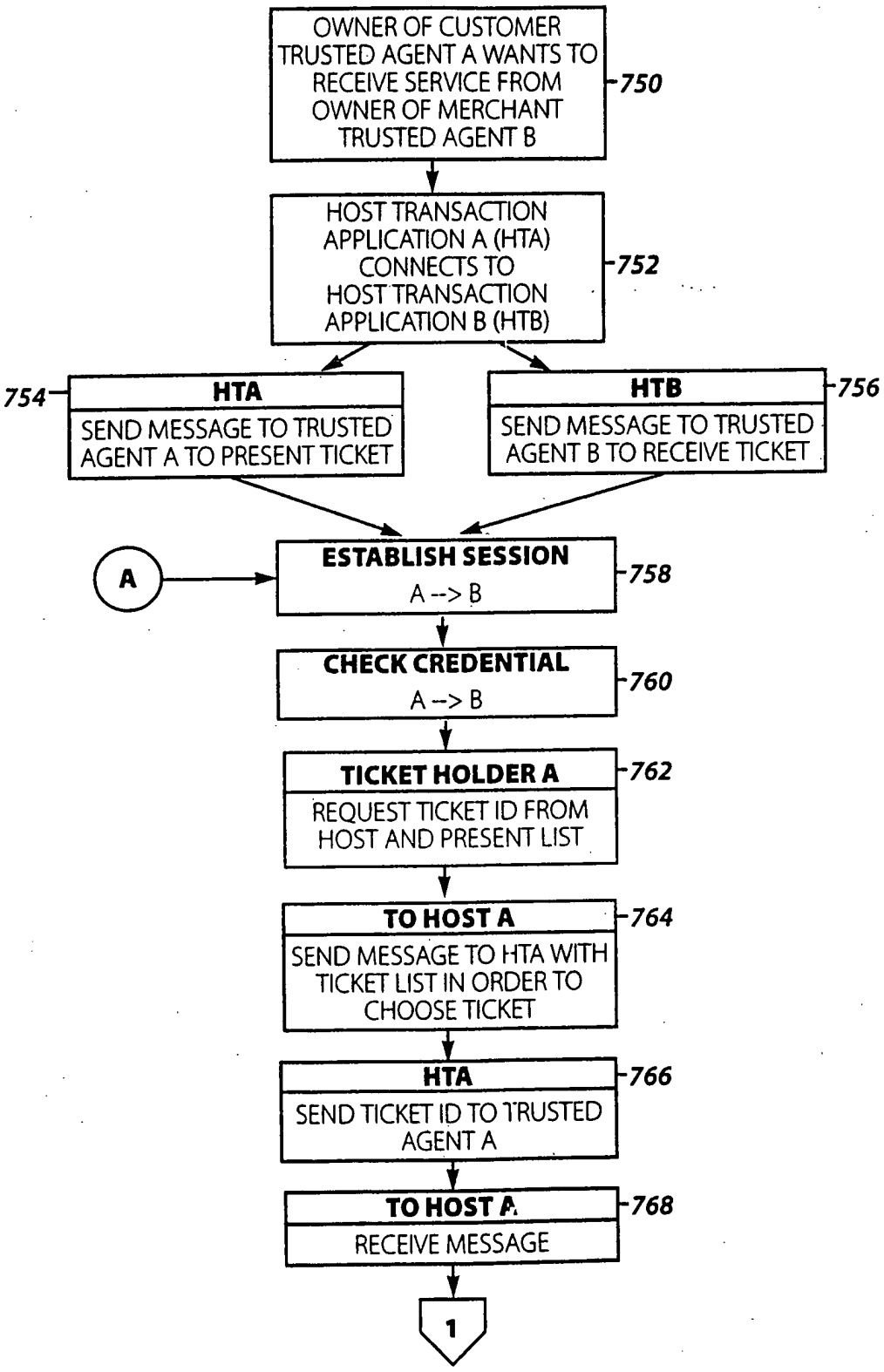
OWNER OF CUSTOMER TRUSTED AGENT A WANTS TO RECEIVE SERVICE FROM OWNER OF MERCHANT TRUSTED AGENT B
750
HOST TRANSACTION APPLICATION A (HTA) CONNECTS TO HOST TRANSACTION APPLICATION B (HTB)
752
754
HTA
SEND MESSAGE TO TRUSTED AGENT A TO PRESENT TICKET
HTB
SEND MESSAGE TO TRUSTED AGENT B TO RECEIVE TICKET
756
A
ESTABLISH SESSION
A --> B
758
CHECK CREDENTIAL
A --> B
760
TICKET HOLDER A
REQUEST TICKET ID FROM HOST AND PRESENT LIST
762
TO HOST A
SEND MESSAGE TO HTA WITH TICKET LIST IN ORDER TO CHOOSE TICKET
764
HTA
SEND TICKET ID TO TRUSTED AGENT A
766
TO HOST A
RECEIVE MESSAGE
768
1

Figure 23A

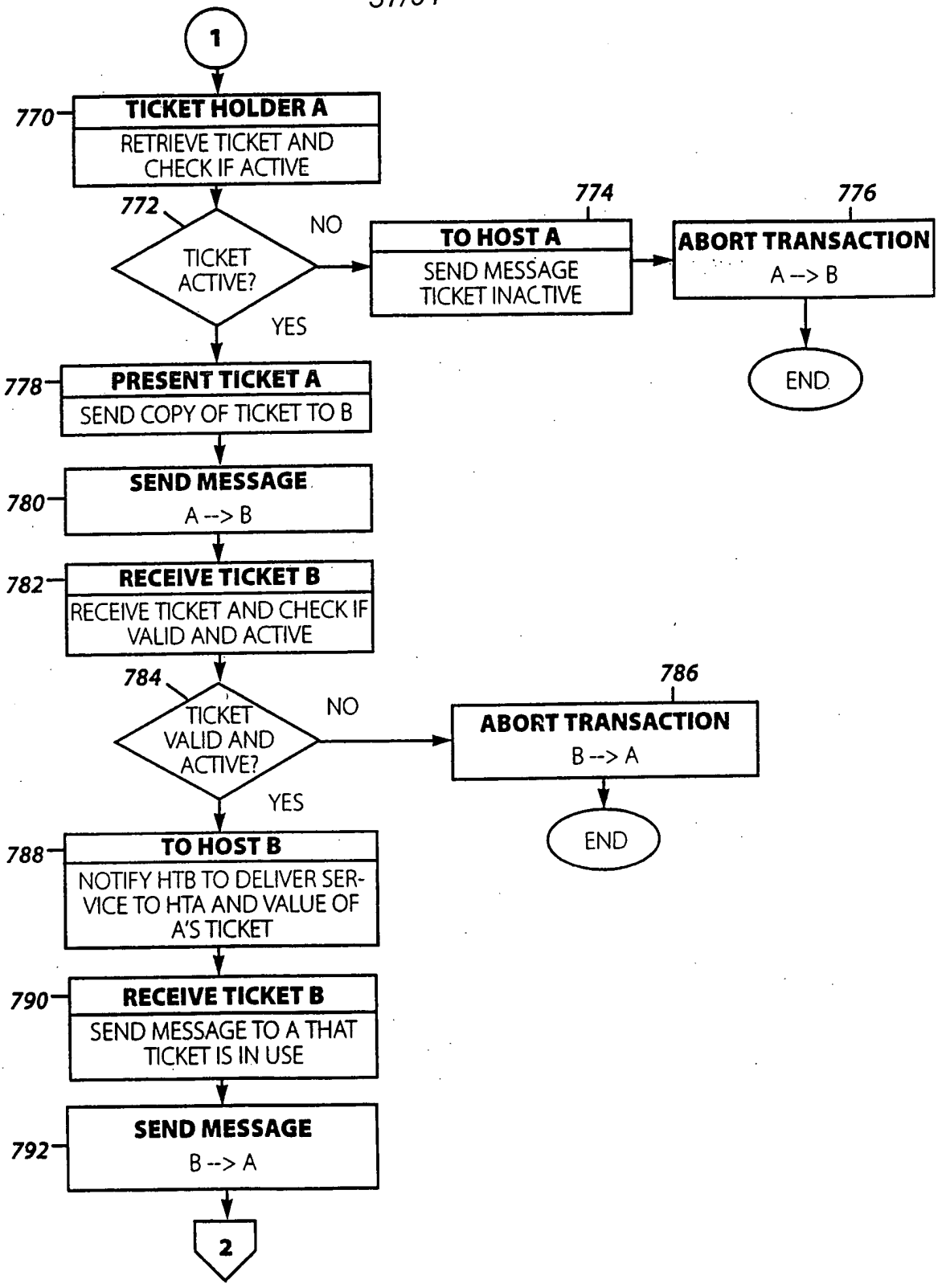
1
770
TICKET HOLDER A
RETRIEVE TICKET AND CHECK IF ACTIVE
772
TICKET ACTIVE?
NO
774
TO HOST A
SEND MESSAGE TICKET INACTIVE
776
ABORT TRANSACTION
A --> B
END
YES
778
PRESENT TICKET A
SEND COPY OF TICKET TO B
780
SEND MESSAGE
A --> B
782
RECEIVE TICKET B
RECEIVE TICKET AND CHECK IF VALID AND ACTIVE
784
TICKET VALID AND ACTIVE?
NO
786
ABORT TRANSACTION
B --> A
END
YES
788
TO HOST B
NOTIFY HTB TO DELIVER SERVICE TO HTA AND VALUE OF A'S TICKET
790
RECEIVE TICKET B
SEND MESSAGE TO A THAT TICKET IS IN USE
792
SEND MESSAGE
B --> A
2

Figure 23B

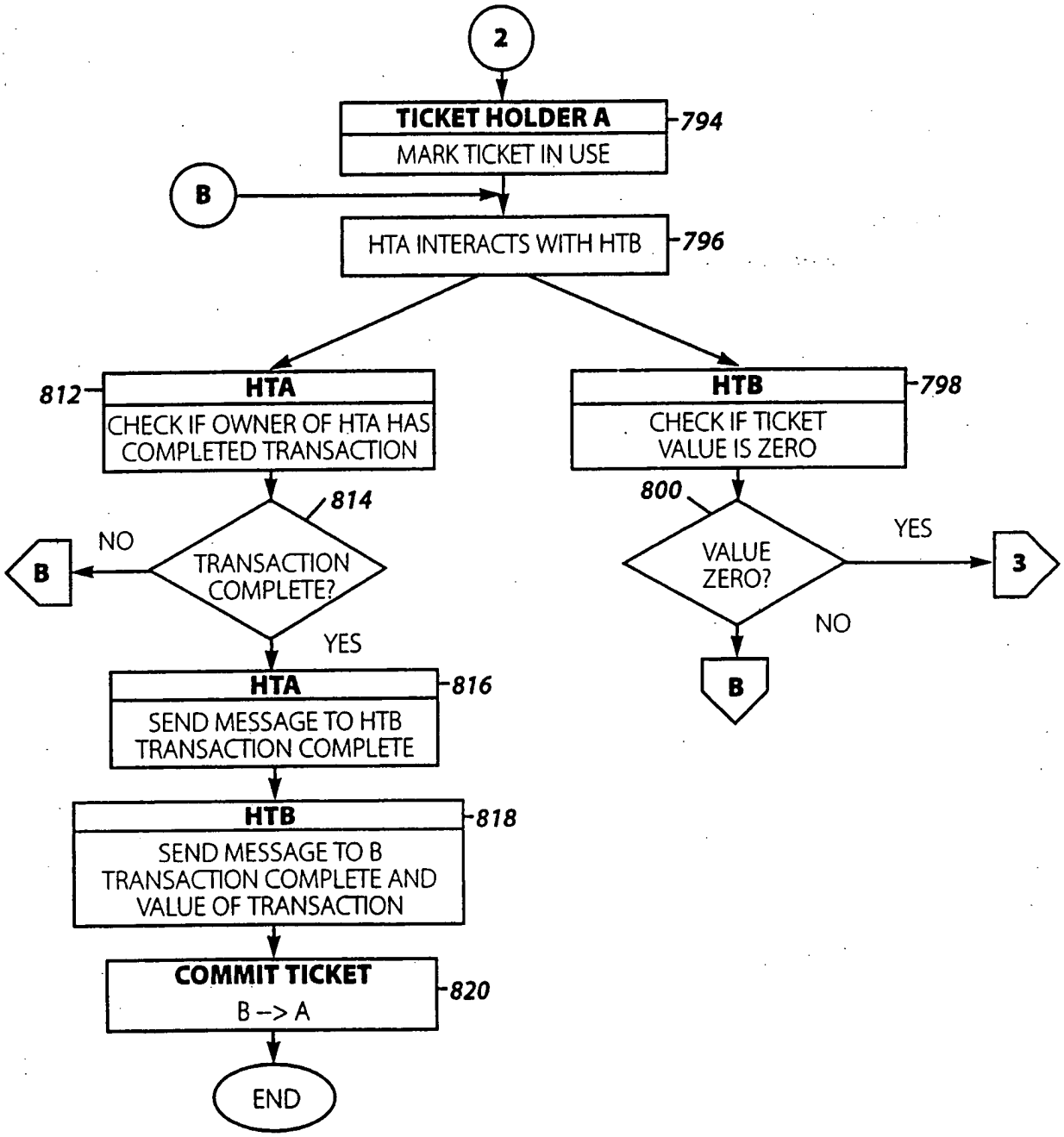
2
TICKET HOLDER A
MARK TICKET IN USE
794
B
HTA INTERACTS WITH HTB
796
812
HTA
CHECK IF OWNER OF HTA HAS COMPLETED TRANSACTION
HTB
CHECK IF TICKET VALUE IS ZERO
798
814
800
NO
B
TRANSACTION COMPLETE?
VALUE ZERO?
YES
3
NO
B
YES
HTA
SEND MESSAGE TO HTB TRANSACTION COMPLETE
816
HTB
SEND MESSAGE TO B TRANSACTION COMPLETE AND VALUE OF TRANSACTION
818
COMMIT TICKET
B –> A
820
END

Figure 23C

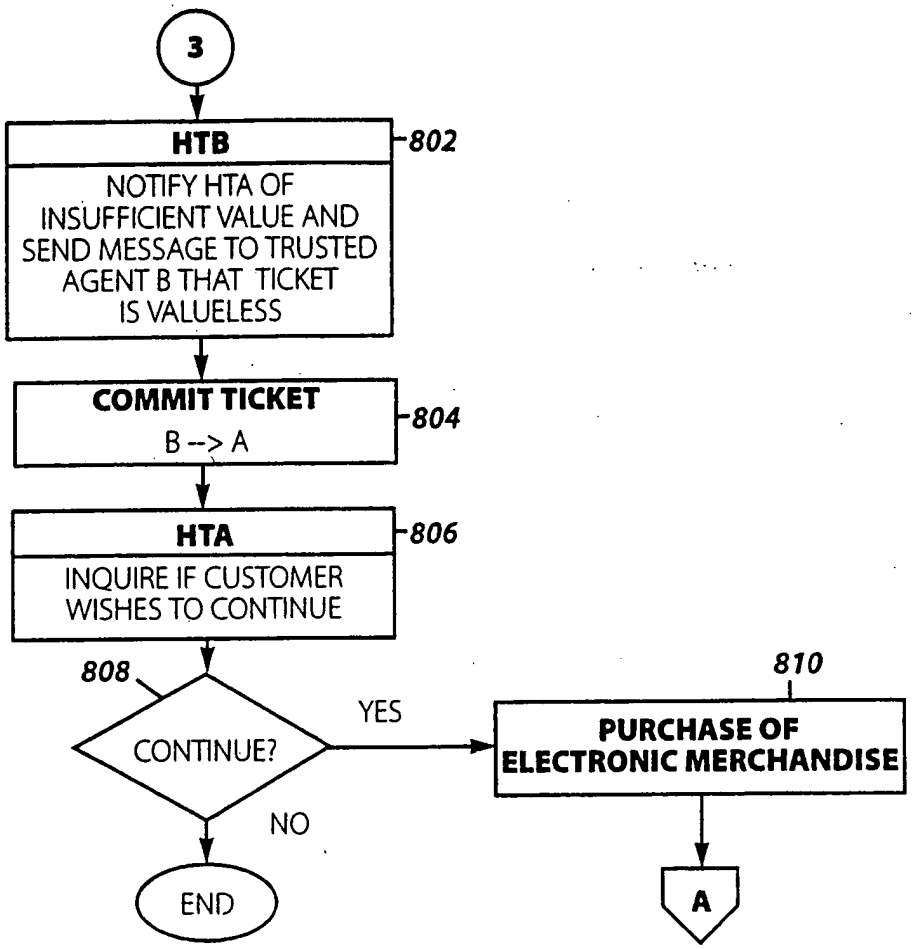
3
HTB
802
NOTIFY HTA OF INSUFFICIENT VALUE AND SEND MESSAGE TO TRUSTED AGENT B THAT TICKET IS VALUELESS
COMMIT TICKET
804
B --> A
HTA
806
INQUIRE IF CUSTOMER WISHES TO CONTINUE
808
CONTINUE?
YES
NO
END
810
PURCHASE OF ELECTRONIC MERCHANDISE
A

Figure 23D

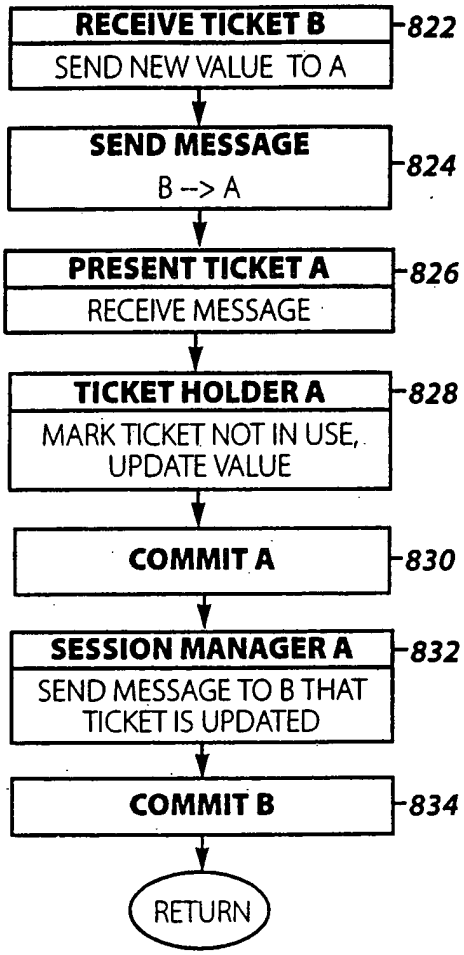
RECEIVE TICKET B
SEND NEW VALUE TO A
822
SEND MESSAGE
B --> A
824
PRESENT TICKET A
RECEIVE MESSAGE
826
TICKET HOLDER A
MARK TICKET NOT IN USE, UPDATE VALUE
828
COMMIT A
830
SESSION MANAGER A
SEND MESSAGE TO B THAT TICKET IS UPDATED
832
COMMIT B
834
RETURN

Figure 24

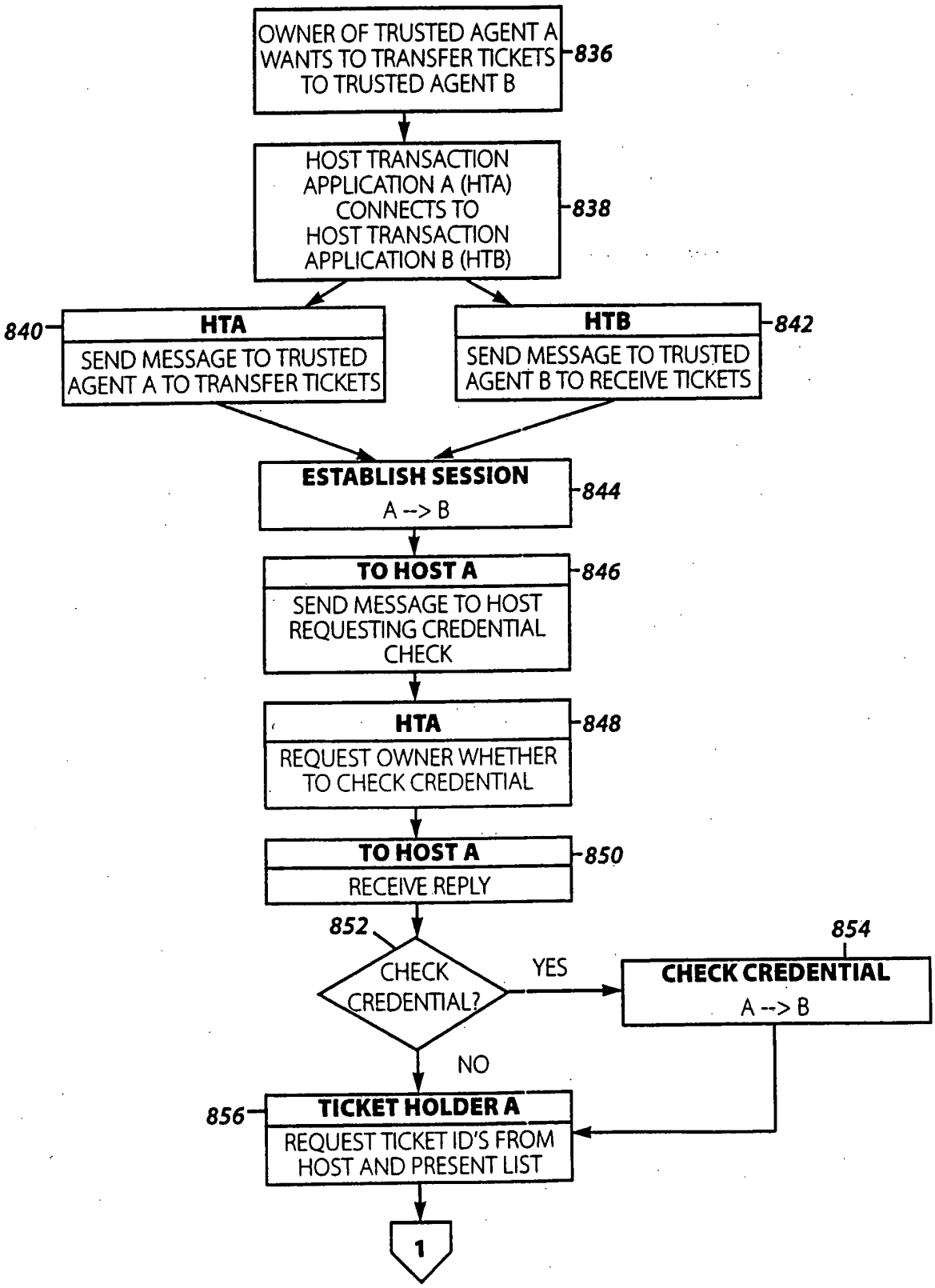
OWNER OF TRUSTED AGENT A WANTS TO TRANSFER TICKETS TO TRUSTED AGENT B
836
HOST TRANSACTION APPLICATION A (HTA) CONNECTS TO HOST TRANSACTION APPLICATION B (HTB)
838
840
HTA
SEND MESSAGE TO TRUSTED AGENT A TO TRANSFER TICKETS
HTB
SEND MESSAGE TO TRUSTED AGENT B TO RECEIVE TICKETS
842
ESTABLISH SESSION
A --> B
844
TO HOST A
SEND MESSAGE TO HOST REQUESTING CREDENTIAL CHECK
846
HTA
REQUEST OWNER WHETHER TO CHECK CREDENTIAL
848
TO HOST A
RECEIVE REPLY
850
852
CHECK CREDENTIAL?
YES
854
CHECK CREDENTIAL
A --> B
NO
856
TICKET HOLDER A
REQUEST TICKET ID'S FROM HOST AND PRESENT LIST
1

Figure 25A

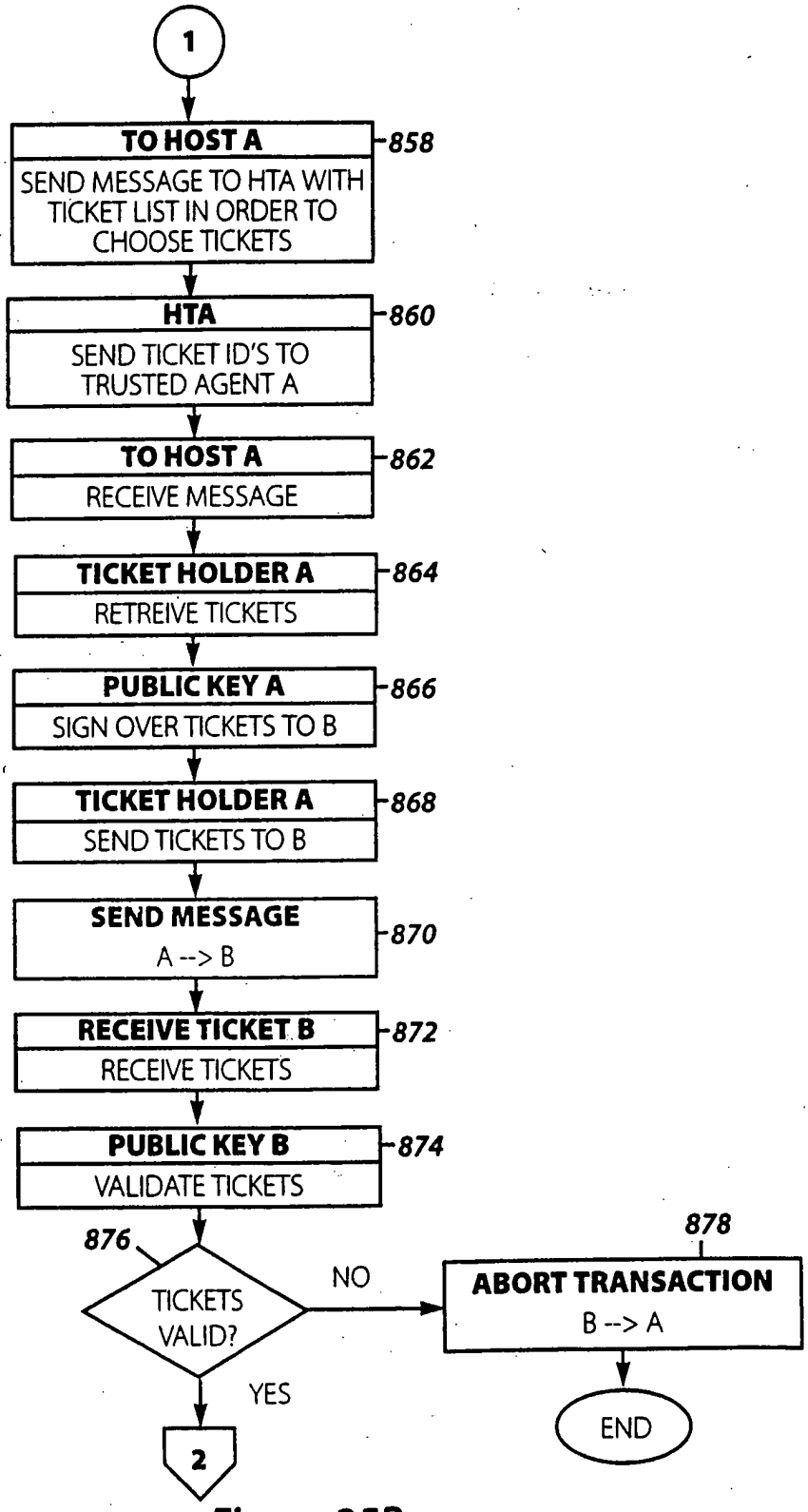
1
TO HOST A
SEND MESSAGE TO HTA WITH TICKET LIST IN ORDER TO CHOOSE TICKETS
858
HTA
SEND TICKET ID'S TO TRUSTED AGENT A
860
TO HOST A
RECEIVE MESSAGE
862
TICKET HOLDER A
RETREIVE TICKETS
864
PUBLIC KEY A
SIGN OVER TICKETS TO B
866
TICKET HOLDER A
SEND TICKETS TO B
868
SEND MESSAGE
A --> B
870
RECEIVE TICKET B
RECEIVE TICKETS
872
PUBLIC KEY B
VALIDATE TICKETS
874
876
TICKETS VALID?
NO
878
ABORT TRANSACTION
B --> A
END
YES
2

Figure 25B

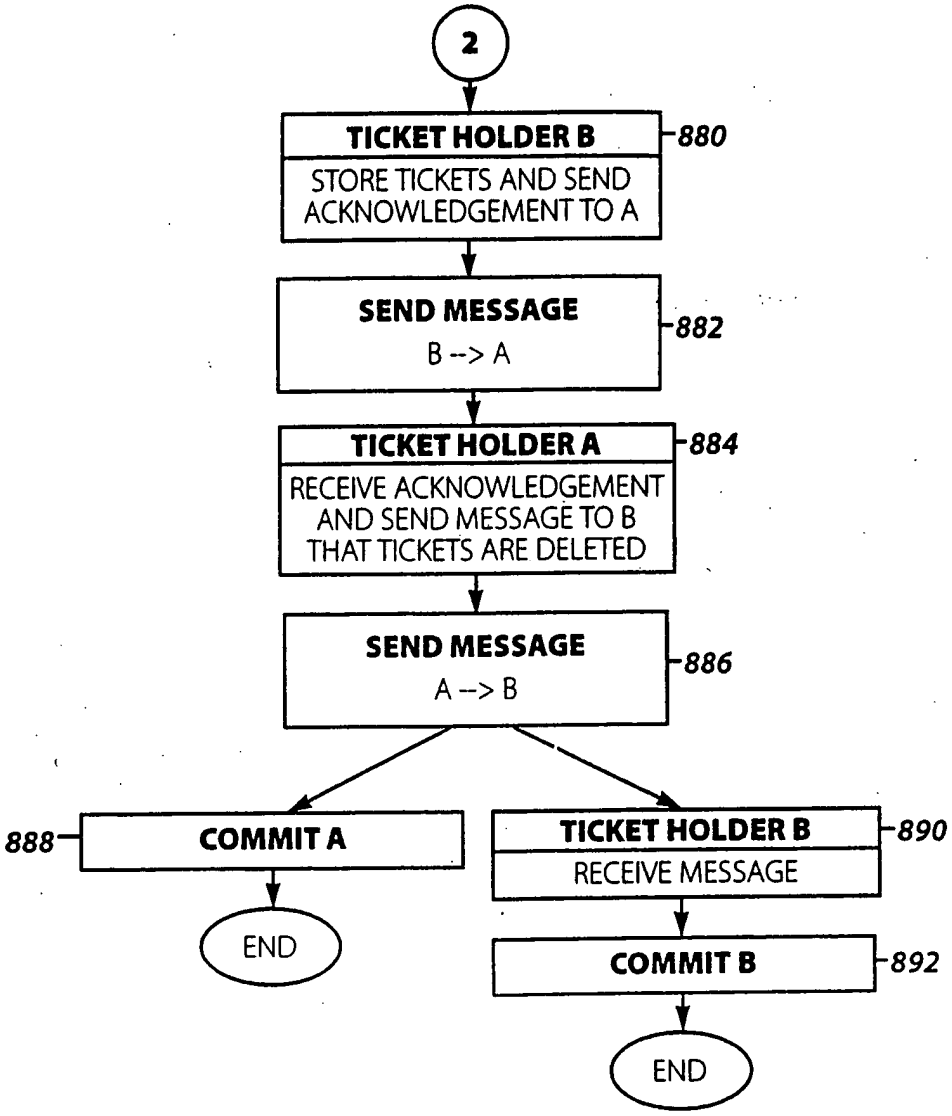
2
TICKET HOLDER B
STORE TICKETS AND SEND ACKNOWLEDGEMENT TO A
880
SEND MESSAGE
B --> A
882
TICKET HOLDER A
RECEIVE ACKNOWLEDGEMENT AND SEND MESSAGE TO B THAT TICKETS ARE DELETED
884
SEND MESSAGE
A --> B
886
888
COMMIT A
END
TICKET HOLDER B
RECEIVE MESSAGE
890
COMMIT B
892
END

Figure 25C

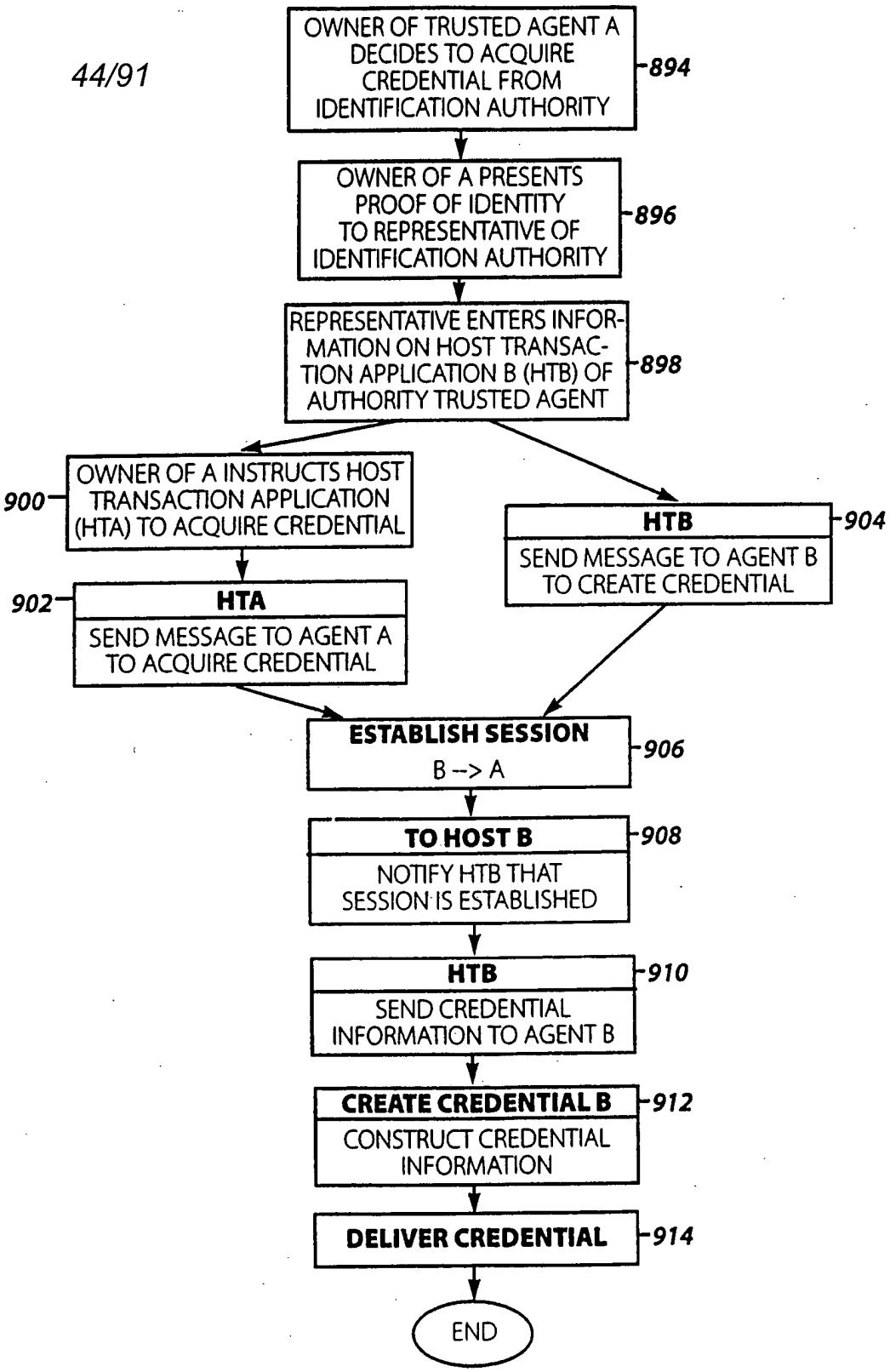
OWNER OF TRUSTED AGENT A DECIDES TO ACQUIRE CREDENTIAL FROM IDENTIFICATION AUTHORITY
894
OWNER OF A PRESENTS PROOF OF IDENTITY TO REPRESENTATIVE OF IDENTIFICATION AUTHORITY
896
REPRESENTATIVE ENTERS INFORMATION ON HOST TRANSACTION APPLICATION B (HTB) OF AUTHORITY TRUSTED AGENT
898
OWNER OF A INSTRUCTS HOST TRANSACTION APPLICATION (HTA) TO ACQUIRE CREDENTIAL
900
HTA
SEND MESSAGE TO AGENT A TO ACQUIRE CREDENTIAL
902
HTB
SEND MESSAGE TO AGENT B TO CREATE CREDENTIAL
904
ESTABLISH SESSION
B --> A
906
TO HOST B
NOTIFY HTB THAT SESSION IS ESTABLISHED
908
HTB
SEND CREDENTIAL INFORMATION TO AGENT B
910
CREATE CREDENTIAL B
CONSTRUCT CREDENTIAL INFORMATION
912
DELIVER CREDENTIAL
914
END

Figure 26

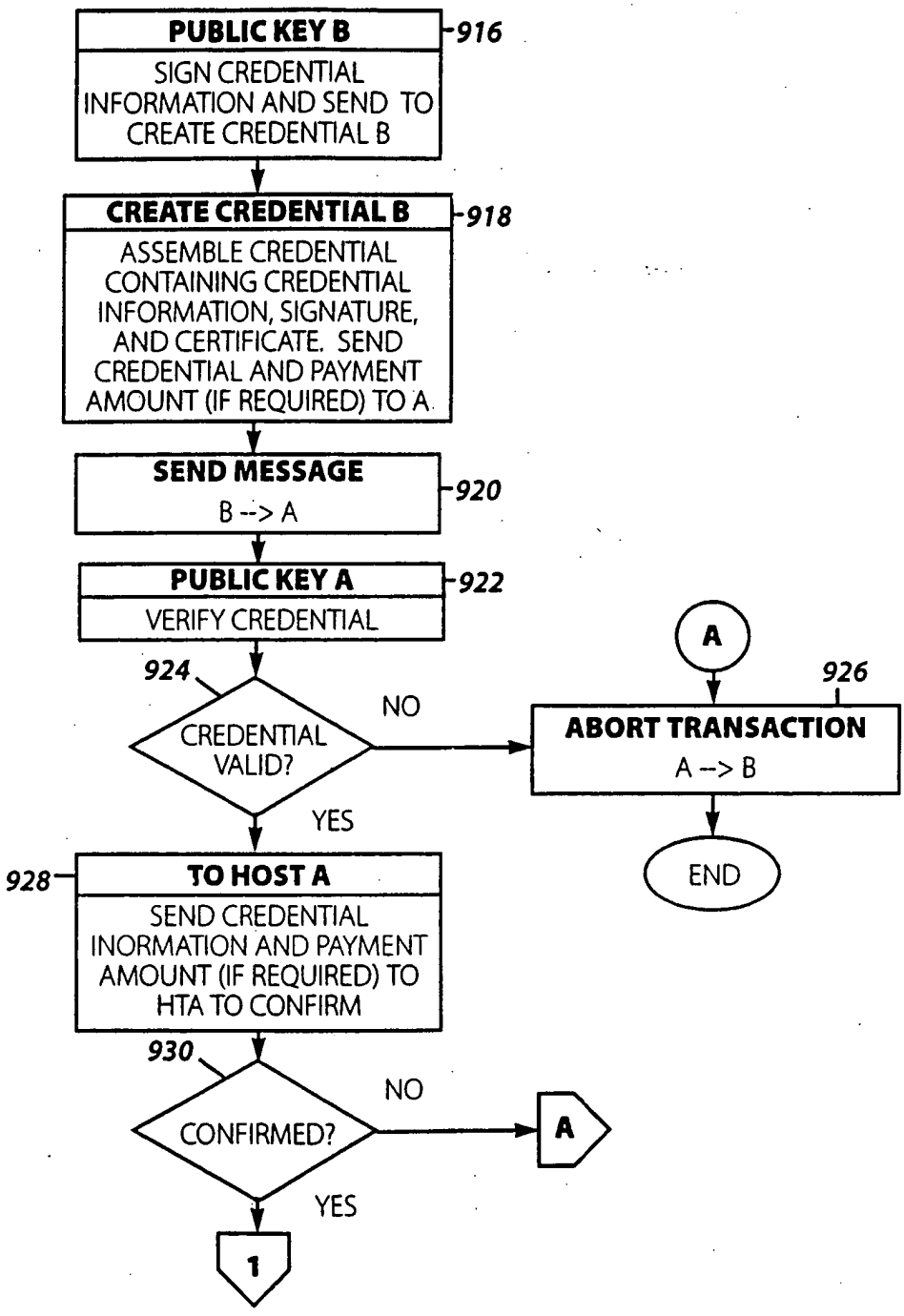
PUBLIC KEY B
916
SIGN CREDENTIAL INFORMATION AND SEND TO CREATE CREDENTIAL B
CREATE CREDENTIAL B
918
ASSEMBLE CREDENTIAL CONTAINING CREDENTIAL INFORMATION, SIGNATURE, AND CERTIFICATE. SEND CREDENTIAL AND PAYMENT AMOUNT (IF REQUIRED) TO A
SEND MESSAGE
B --> A
920
PUBLIC KEY A
922
VERIFY CREDENTIAL
924
CREDENTIAL VALID?
NO
YES
A
926
ABORT TRANSACTION
A --> B
END
928
TO HOST A
SEND CREDENTIAL INORMATION AND PAYMENT AMOUNT (IF REQUIRED) TO HTA TO CONFIRM
930
CONFIRMED?
NO
A
YES
1

Figure 27A

46/91

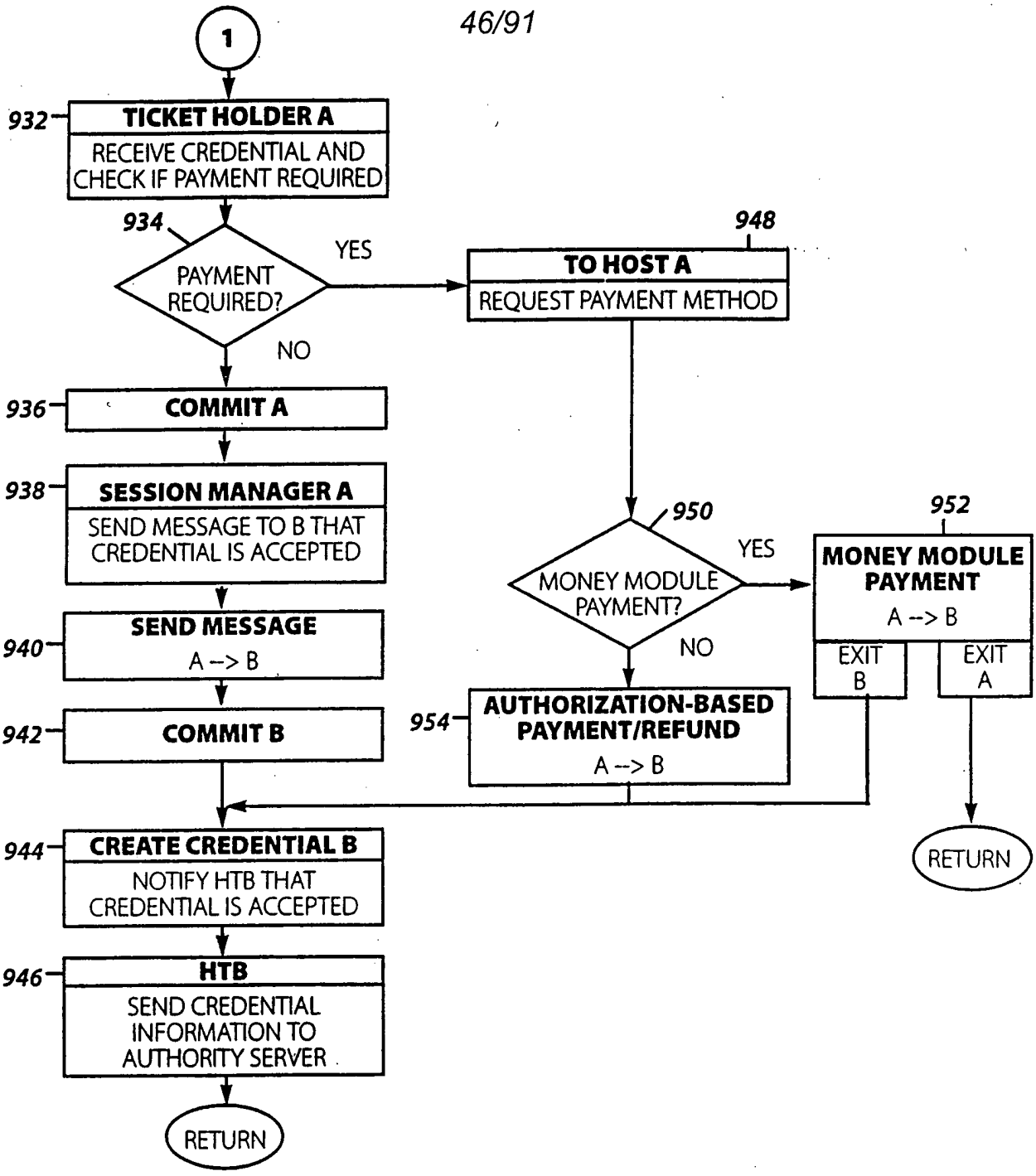

Figure 27B

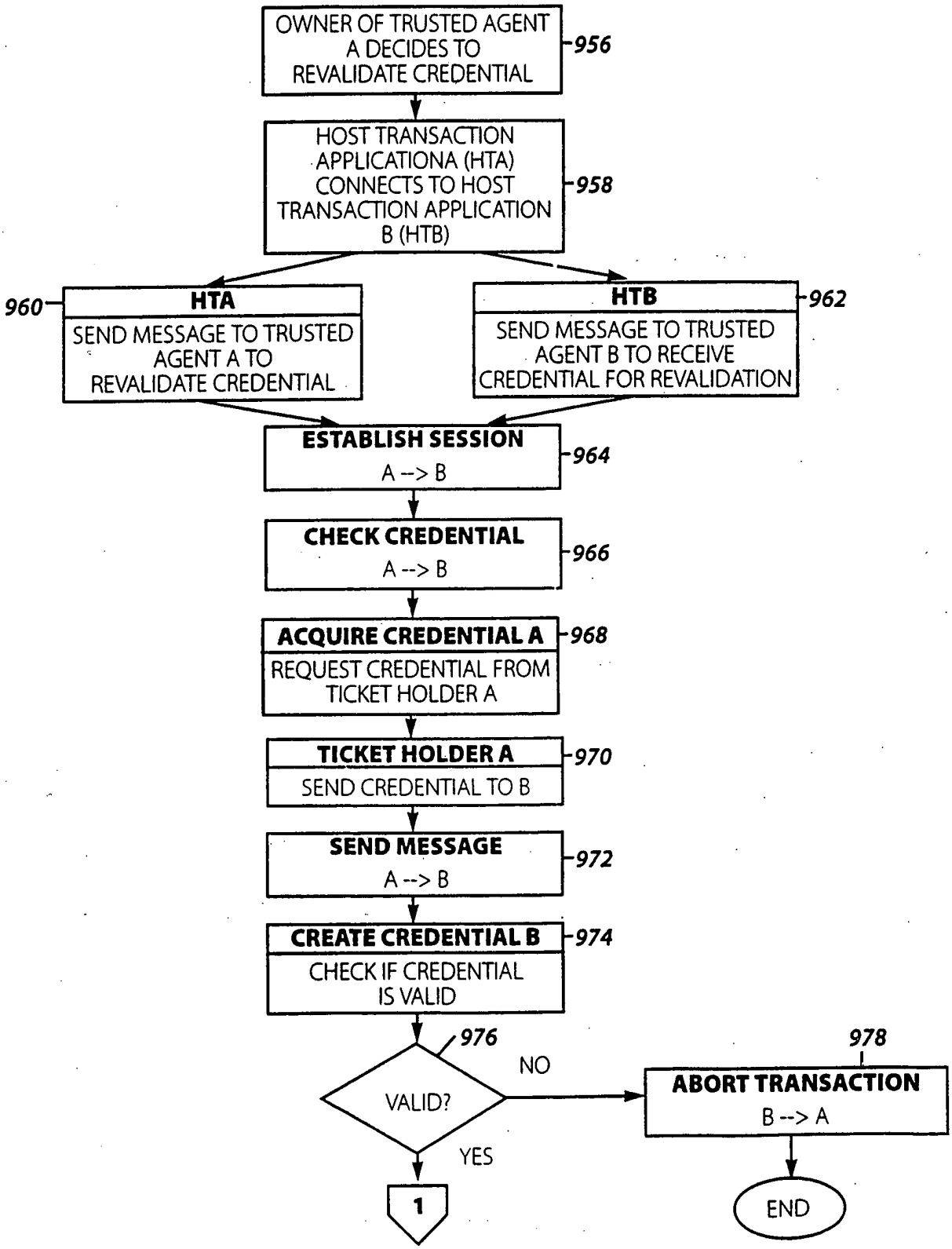
OWNER OF TRUSTED AGENT A DECIDES TO REVALIDATE CREDENTIAL
956
HOST TRANSACTION APPLICATIONA (HTA) CONNECTS TO HOST TRANSACTION APPLICATION B (HTB)
958
960
HTA
SEND MESSAGE TO TRUSTED AGENT A TO REVALIDATE CREDENTIAL
HTB
SEND MESSAGE TO TRUSTED AGENT B TO RECEIVE CREDENTIAL FOR REVALIDATION
962
ESTABLISH SESSION
A --> B
964
CHECK CREDENTIAL
A --> B
966
ACQUIRE CREDENTIAL A
REQUEST CREDENTIAL FROM TICKET HOLDER A
968
TICKET HOLDER A
SEND CREDENTIAL TO B
970
SEND MESSAGE
A --> B
972
CREATE CREDENTIAL B
CHECK IF CREDENTIAL IS VALID
974
976
VALID?
NO
YES
978
ABORT TRANSACTION
B --> A
1
END

Figure 28A

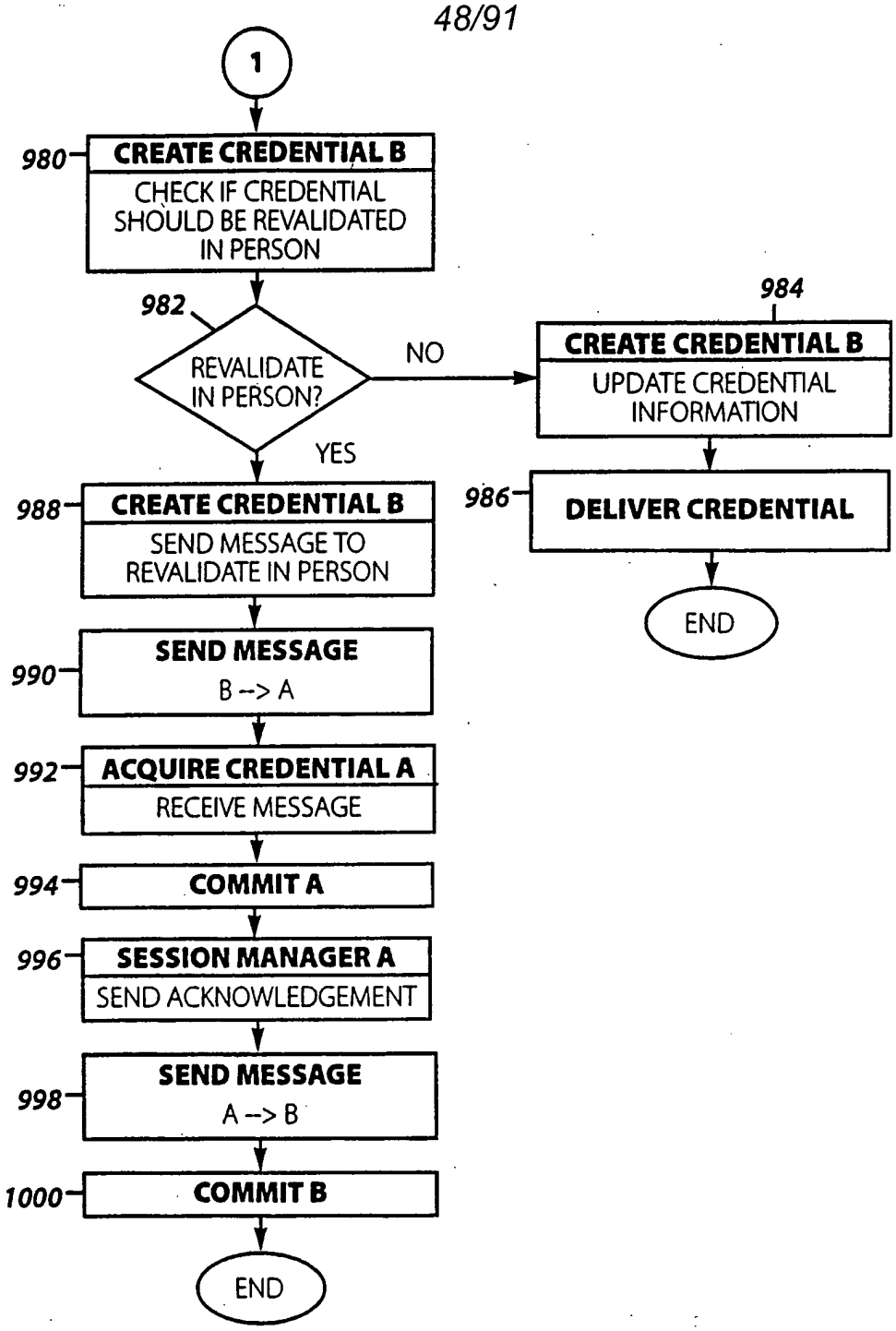
1
980
CREATE CREDENTIAL B
CHECK IF CREDENTIAL SHOULD BE REVALIDATED IN PERSON
982
REVALIDATE IN PERSON?
NO
984
CREATE CREDENTIAL B
UPDATE CREDENTIAL INFORMATION
YES
988
CREATE CREDENTIAL B
SEND MESSAGE TO REVALIDATE IN PERSON
986
DELIVER CREDENTIAL
END
990
SEND MESSAGE
B --> A
992
ACQUIRE CREDENTIAL A
RECEIVE MESSAGE
994
COMMIT A
996
SESSION MANAGER A
SEND ACKNOWLEDGEMENT
998
SEND MESSAGE
A --> B
1000
COMMIT B
END

Figure 28B

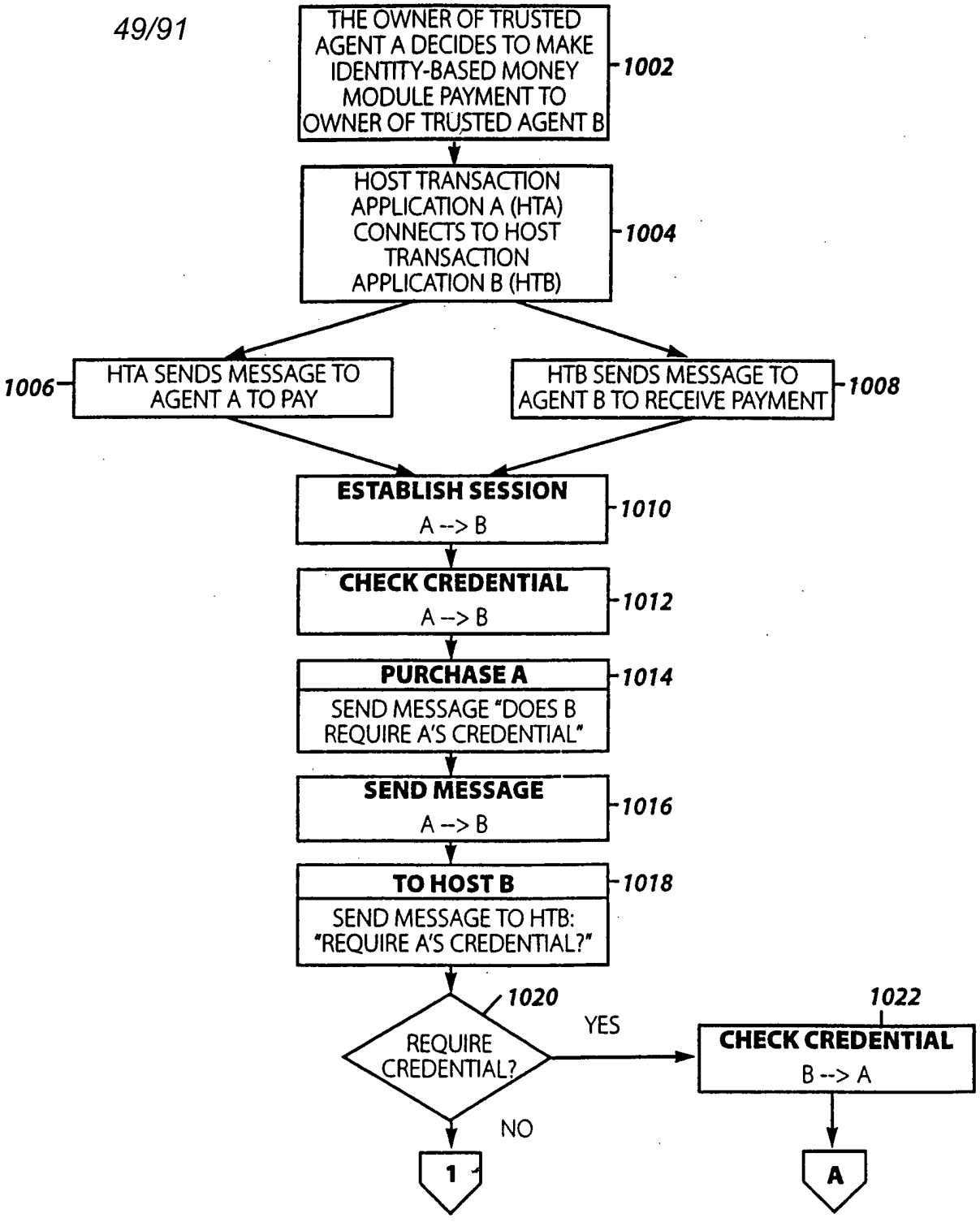
THE OWNER OF TRUSTED AGENT A DECIDES TO MAKE IDENTITY-BASED MONEY MODULE PAYMENT TO OWNER OF TRUSTED AGENT B
1002
HOST TRANSACTION APPLICATION A (HTA) CONNECTS TO HOST TRANSACTION APPLICATION B (HTB)
1004
1006
HTA SENDS MESSAGE TO AGENT A TO PAY
HTB SENDS MESSAGE TO AGENT B TO RECEIVE PAYMENT
1008
ESTABLISH SESSION
A --> B
1010
CHECK CREDENTIAL
A --> B
1012
PURCHASE A
SEND MESSAGE "DOES B REQUIRE A'S CREDENTIAL"
1014
SEND MESSAGE
A --> B
1016
TO HOST B
SEND MESSAGE TO HTB: "REQUIRE A'S CREDENTIAL?"
1018
1020
REQUIRE CREDENTIAL?
YES
1022
CHECK CREDENTIAL
B --> A
NO
1
A

Figure 29A

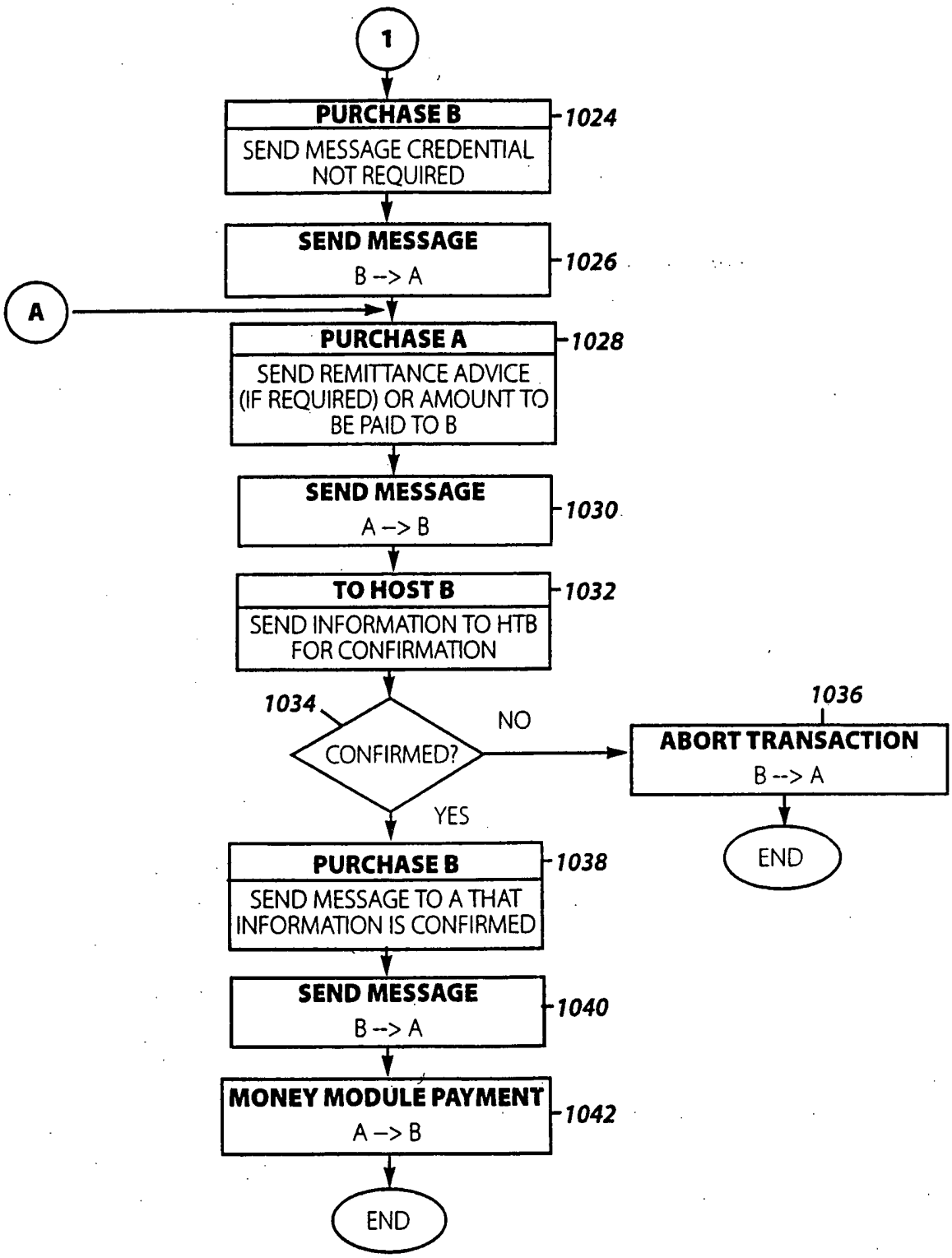
1
PURCHASE B
SEND MESSAGE CREDENTIAL NOT REQUIRED
1024
SEND MESSAGE
B --> A
1026
A
PURCHASE A
SEND REMITTANCE ADVICE (IF REQUIRED) OR AMOUNT TO BE PAID TO B
1028
SEND MESSAGE
A --> B
1030
TO HOST B
SEND INFORMATION TO HTB FOR CONFIRMATION
1032
1034
CONFIRMED?
NO
1036
ABORT TRANSACTION
B --> A
END
YES
PURCHASE B
SEND MESSAGE TO A THAT INFORMATION IS CONFIRMED
1038
SEND MESSAGE
B --> A
1040
MONEY MODULE PAYMENT
A --> B
1042
END

Figure 29B

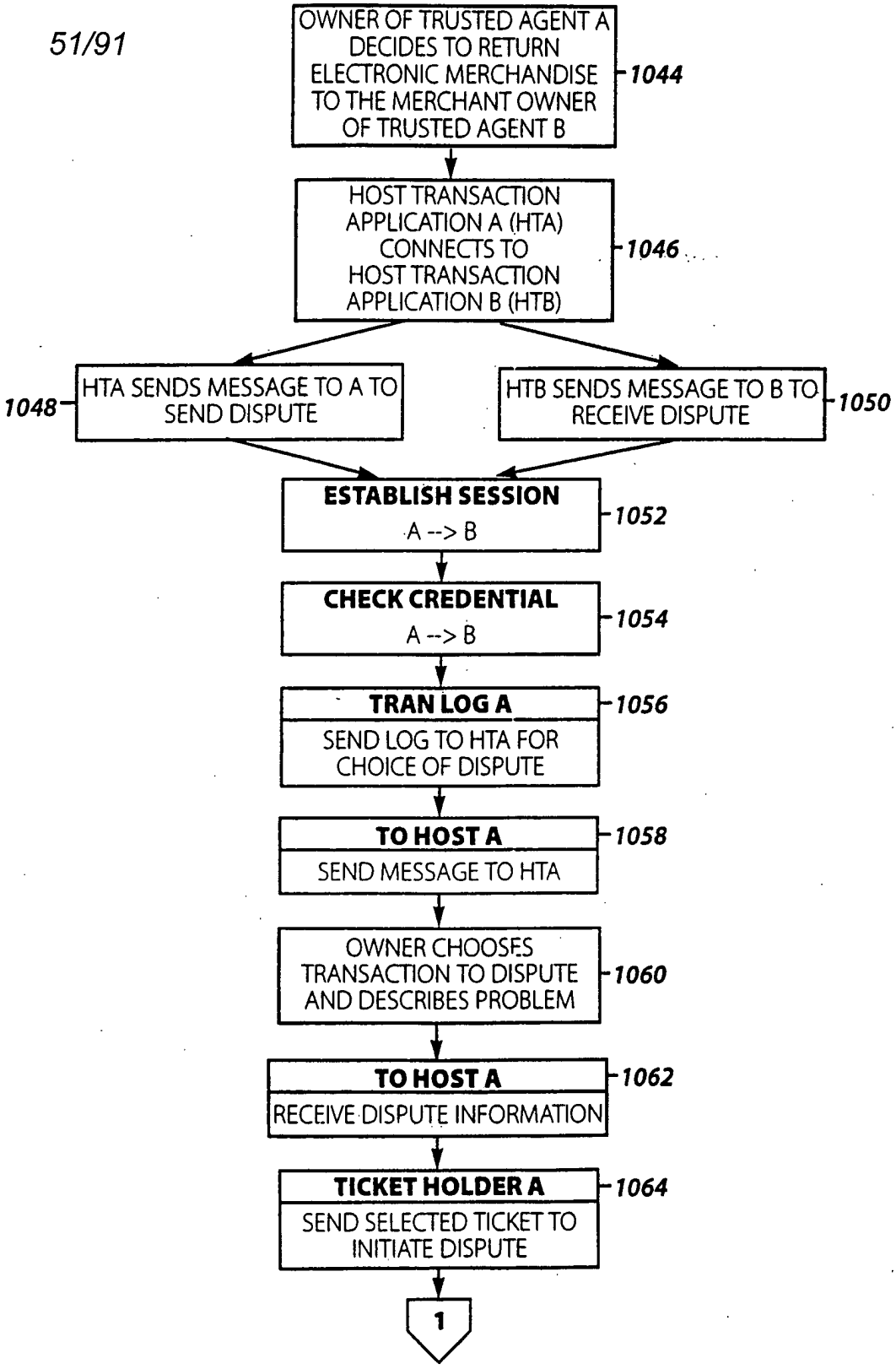
OWNER OF TRUSTED AGENT A DECIDES TO RETURN ELECTRONIC MERCHANDISE TO THE MERCHANT OWNER OF TRUSTED AGENT B
1044
HOST TRANSACTION APPLICATION A (HTA) CONNECTS TO HOST TRANSACTION APPLICATION B (HTB)
1046
1048
HTA SENDS MESSAGE TO A TO SEND DISPUTE
HTB SENDS MESSAGE TO B TO RECEIVE DISPUTE
1050
ESTABLISH SESSION
A --> B
1052
CHECK CREDENTIAL
A --> B
1054
TRAN LOG A
SEND LOG TO HTA FOR CHOICE OF DISPUTE
1056
TO HOST A
SEND MESSAGE TO HTA
1058
OWNER CHOOSES TRANSACTION TO DISPUTE AND DESCRIBES PROBLEM
1060
TO HOST A
RECEIVE DISPUTE INFORMATION
1062
TICKET HOLDER A
SEND SELECTED TICKET TO INITIATE DISPUTE
1064
1

Figure 30A

52/91

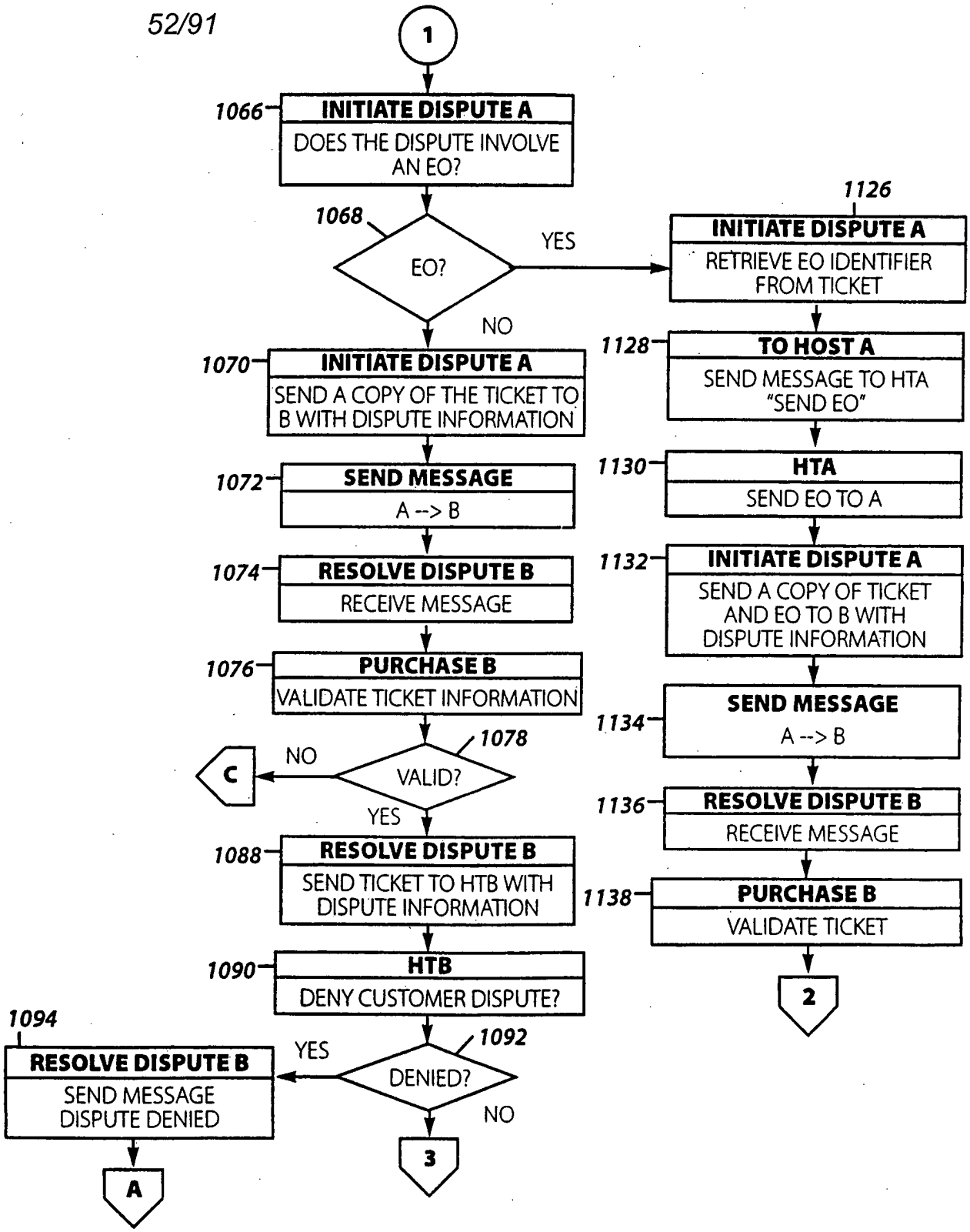

Figure 30B

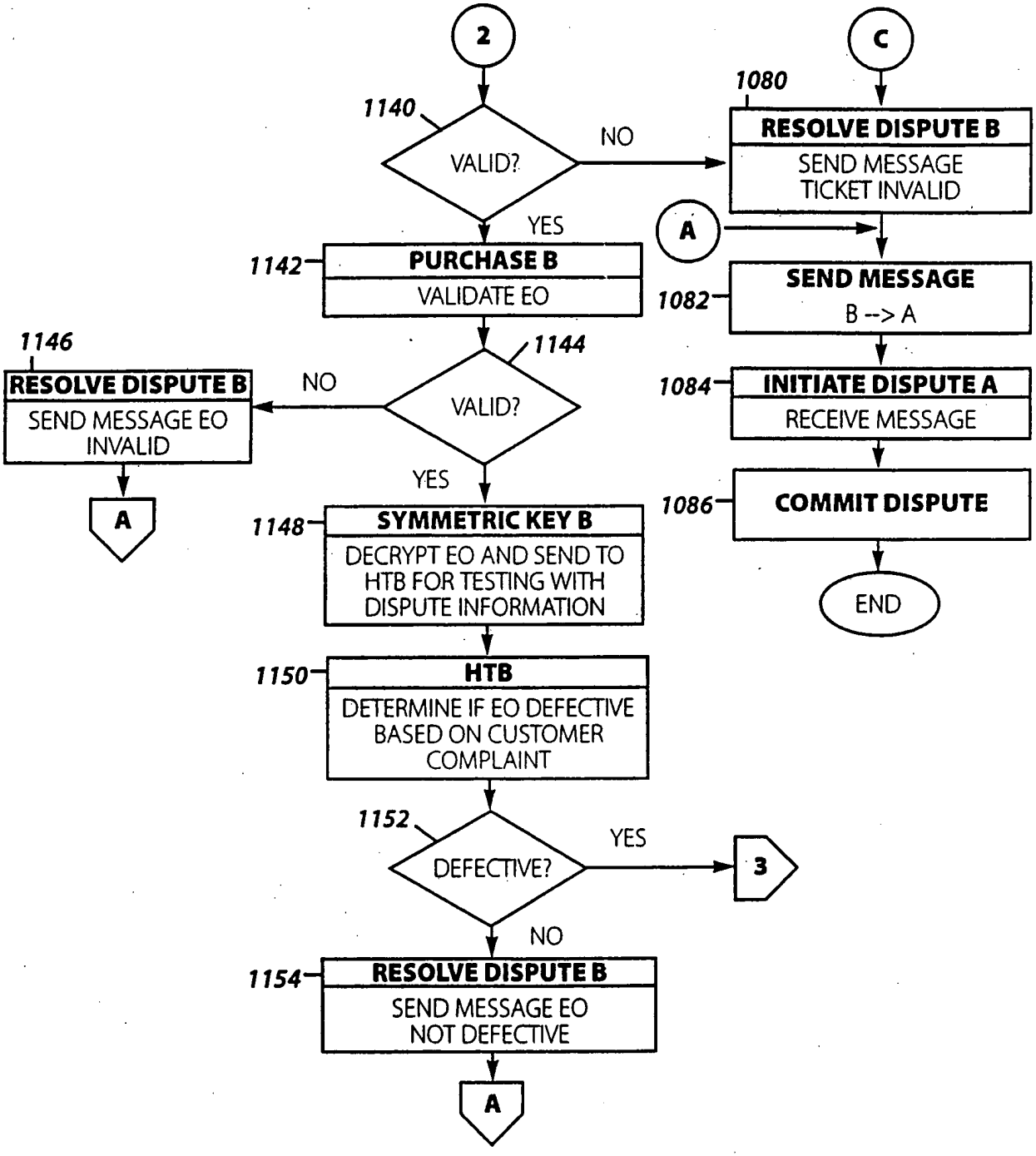
2
C
1080
1140
VALID?
NO
RESOLVE DISPUTE B
SEND MESSAGE
TICKET INVALID
YES
A
1142
PURCHASE B
VALIDATE EO
SEND MESSAGE
1082
B --> A
1146
1144
RESOLVE DISPUTE B
SEND MESSAGE EO
INVALID
NO
VALID?
1084
INITIATE DISPUTE A
RECEIVE MESSAGE
YES
A
1148
SYMMETRIC KEY B
DECRYPT EO AND SEND TO
HTB FOR TESTING WITH
DISPUTE INFORMATION
1086
COMMIT DISPUTE
END
1150
HTB
DETERMINE IF EO DEFECTIVE
BASED ON CUSTOMER
COMPLAINT
1152
DEFECTIVE?
YES
3
NO
1154
RESOLVE DISPUTE B
SEND MESSAGE EO
NOT DEFECTIVE
A

Figure 30C

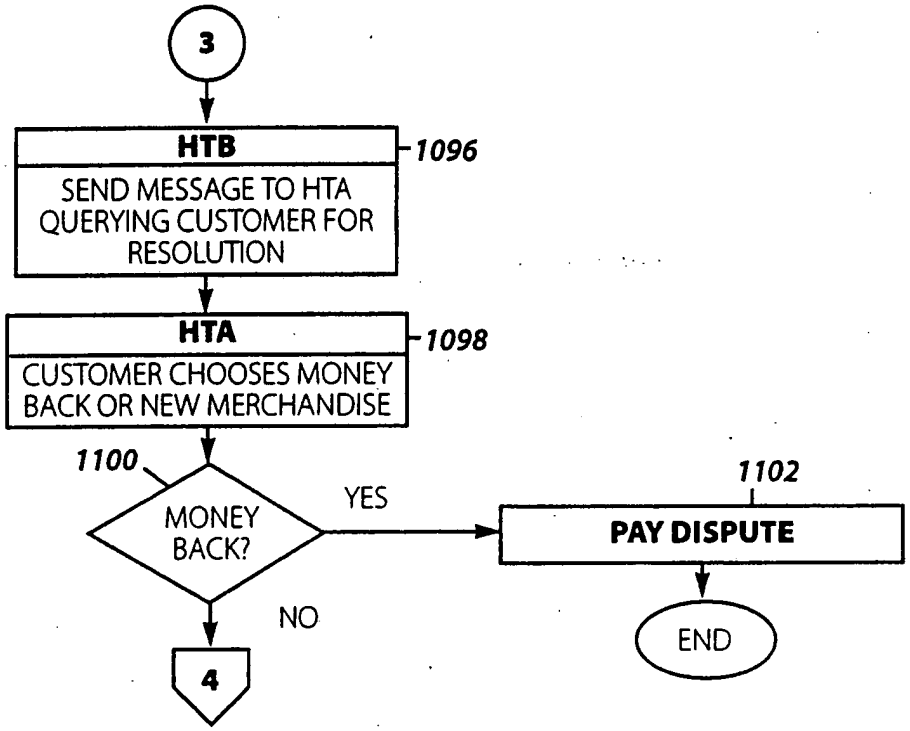
3
HTB
1096
SEND MESSAGE TO HTA QUERYING CUSTOMER FOR RESOLUTION
HTA
1098
CUSTOMER CHOOSES MONEY BACK OR NEW MERCHANDISE
1100
MONEY BACK?
YES
1102
PAY DISPUTE
END
NO
4

Figure 30D

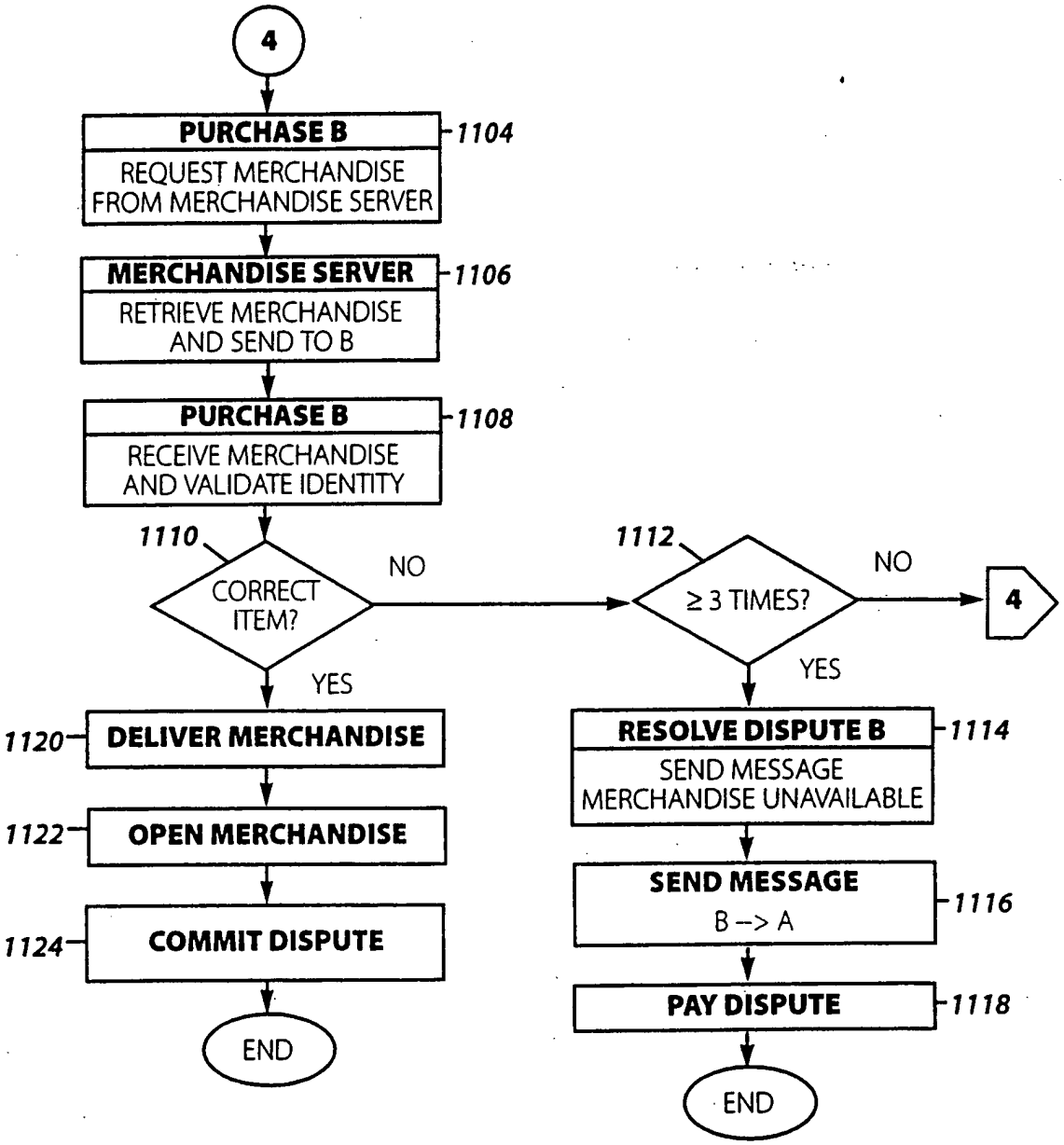
4
PURCHASE B
REQUEST MERCHANDISE FROM MERCHANDISE SERVER
1104
MERCHANDISE SERVER
RETRIEVE MERCHANDISE AND SEND TO B
1106
PURCHASE B
RECEIVE MERCHANDISE AND VALIDATE IDENTITY
1108
1110
CORRECT ITEM?
NO
YES
1112
≥ 3 TIMES?
NO
4
YES
1120
DELIVER MERCHANDISE
1122
OPEN MERCHANDISE
1124
COMMIT DISPUTE
END
RESOLVE DISPUTE B
SEND MESSAGE MERCHANDISE UNAVAILABLE
1114
SEND MESSAGE
B –> A
1116
PAY DISPUTE
1118
END

Figure 30E

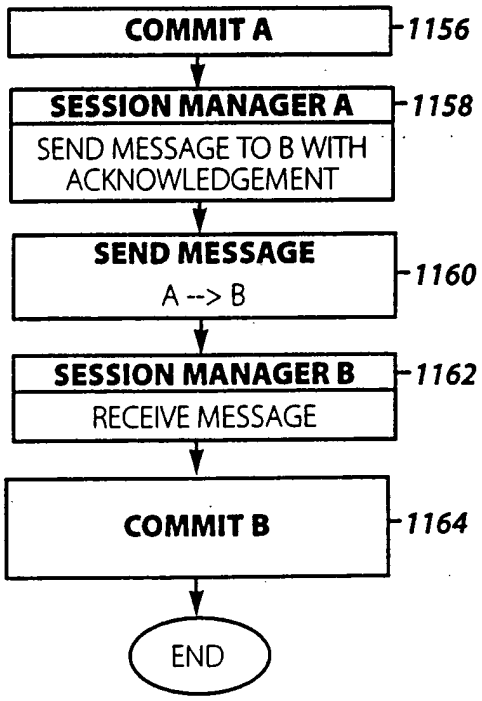
COMMIT A
1156
SESSION MANAGER A
1158
SEND MESSAGE TO B WITH ACKNOWLEDGEMENT
SEND MESSAGE
A --> B
1160
SESSION MANAGER B
1162
RECEIVE MESSAGE
COMMIT B
1164
END

Figure 31

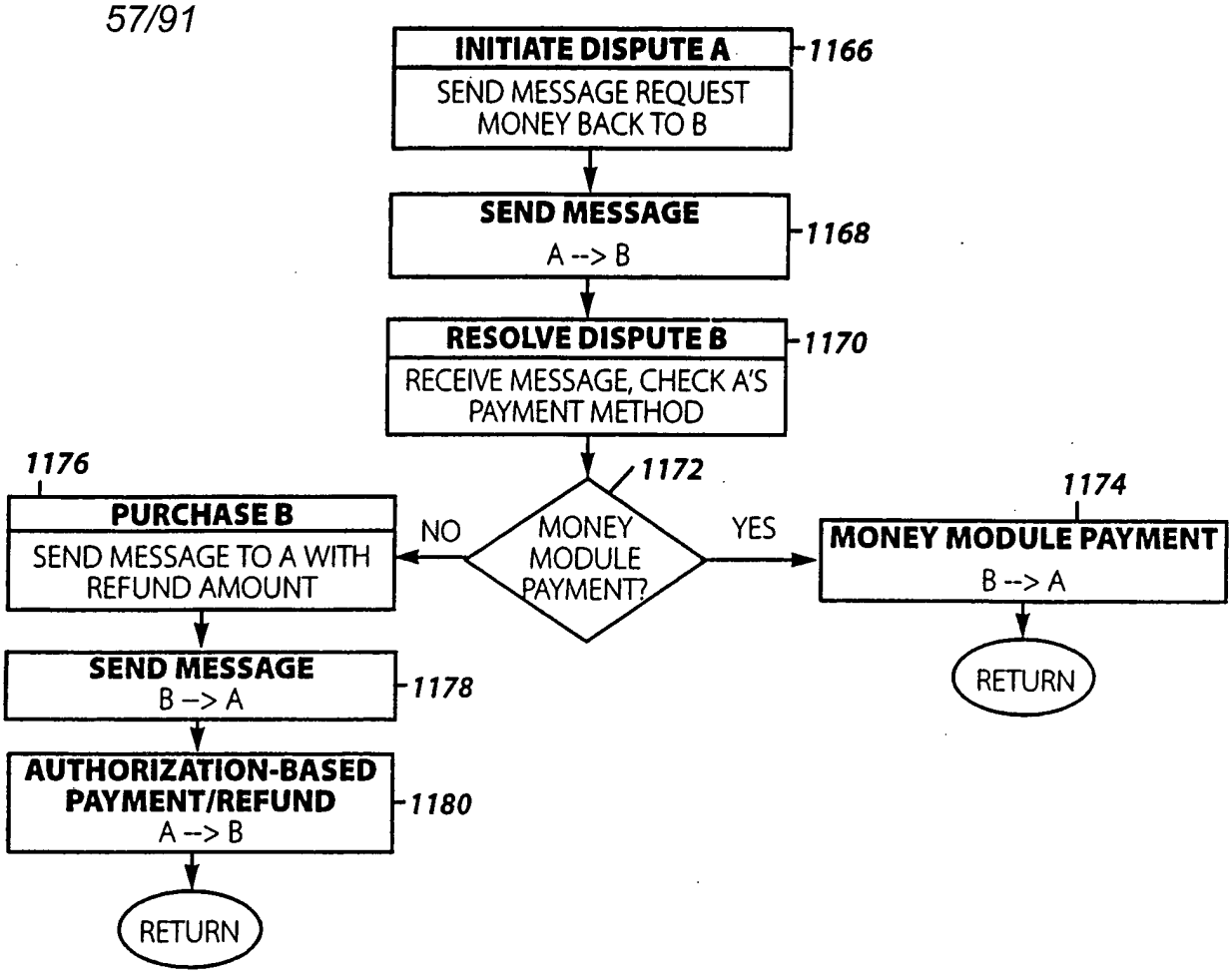
INITIATE DISPUTE A
SEND MESSAGE REQUEST MONEY BACK TO B
1166
SEND MESSAGE
A --> B
1168
RESOLVE DISPUTE B
RECEIVE MESSAGE, CHECK A'S PAYMENT METHOD
1170
1172
MONEY MODULE PAYMENT?
NO
YES
1176
PURCHASE B
SEND MESSAGE TO A WITH REFUND AMOUNT
1174
MONEY MODULE PAYMENT
B --> A
RETURN
SEND MESSAGE
B --> A
1178
AUTHORIZATION-BASED PAYMENT/REFUND
A --> B
1180
RETURN

Figure 32

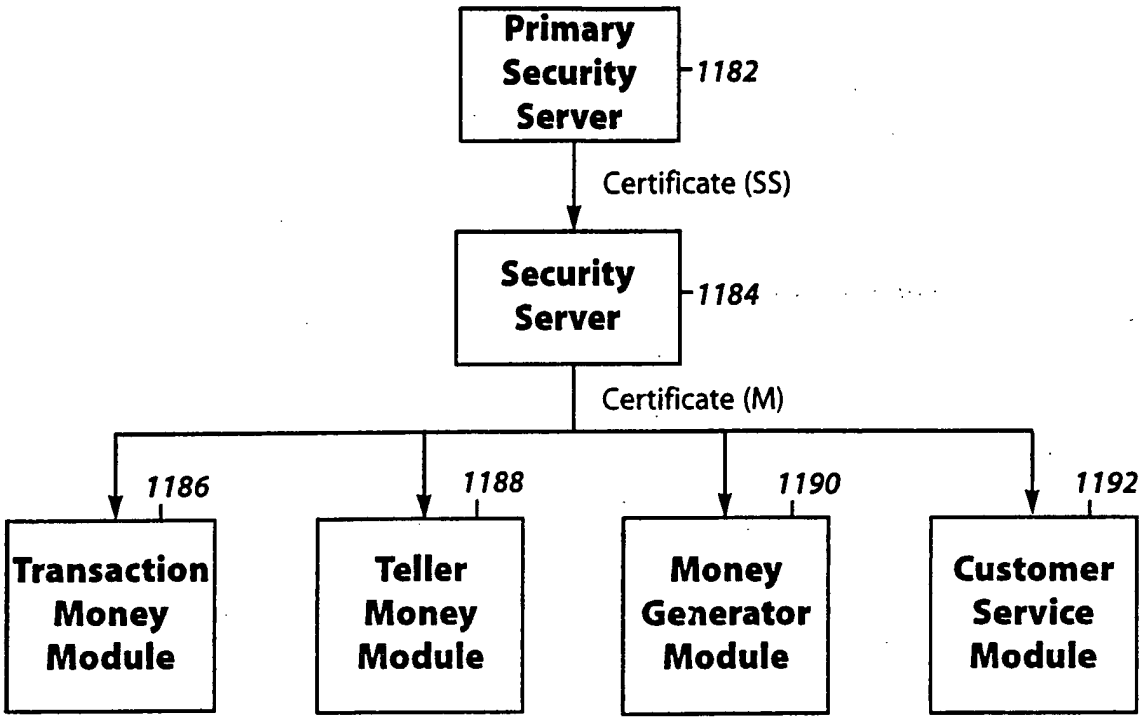

Figure 33A

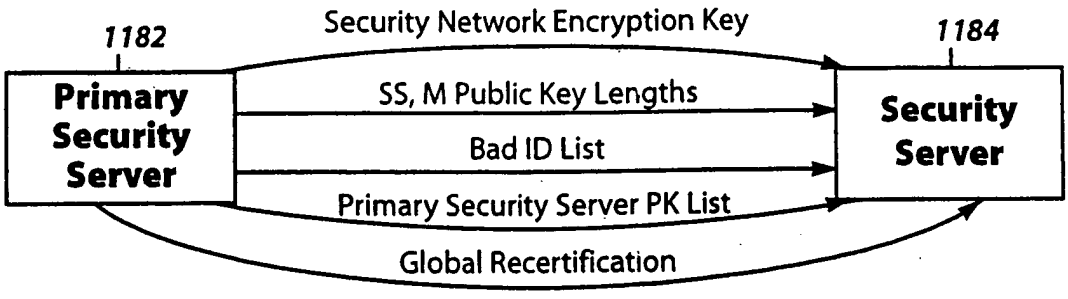

Figure 33B

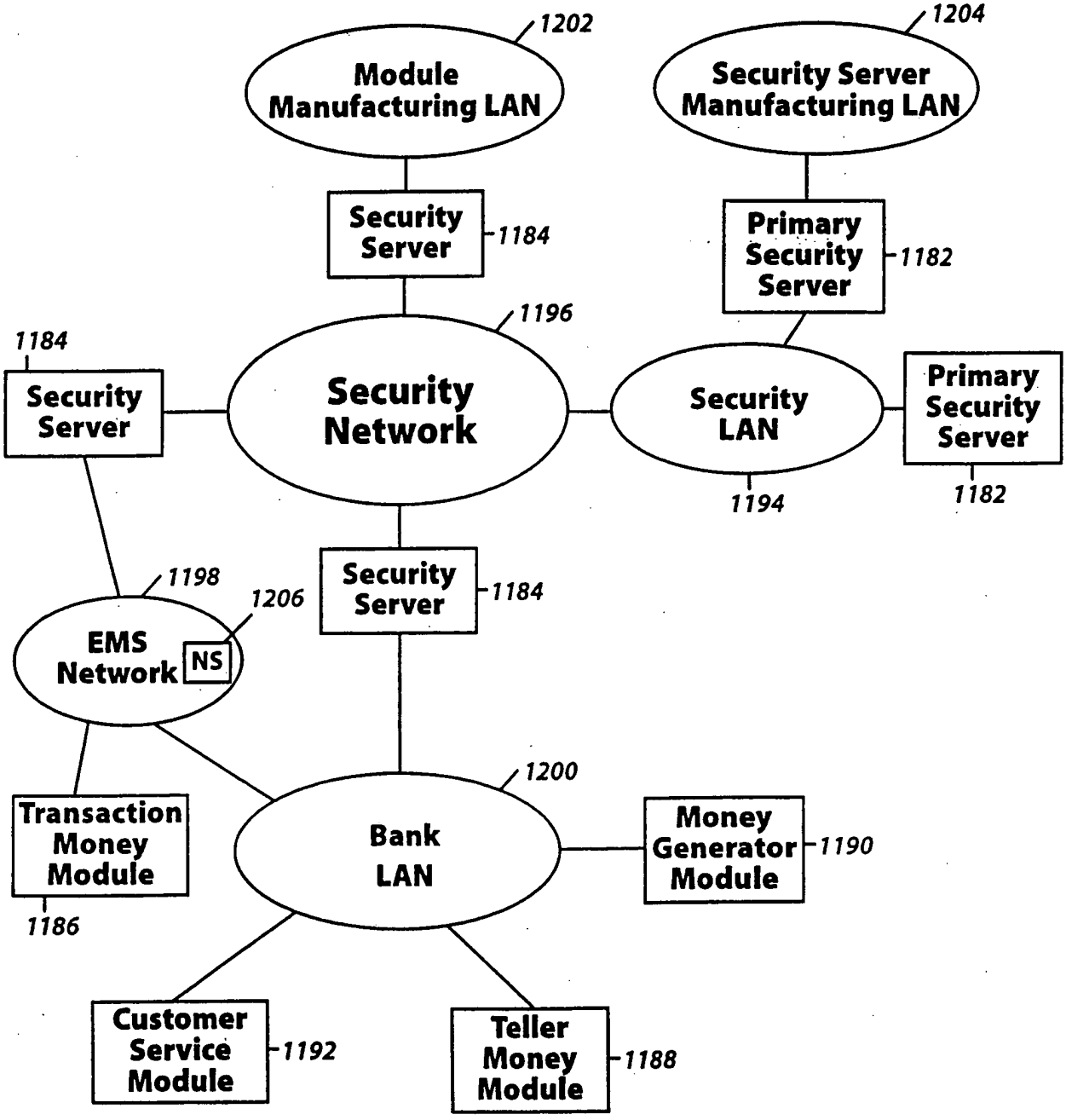
1202
Module Manufacturing LAN
1204
Security Server Manufacturing LAN
Security Server
1184
Primary Security Server
1182
1196
1184
Security Server
Security Network
Security LAN
Primary Security Server
1194
1182
1198
1206
Security Server
1184
EMS Network
NS
1200
Transaction Money Module
1186
Bank LAN
Money Generator Module
1190
Customer Service Module
1192
Teller Money Module
1188

Figure 34

Security Server

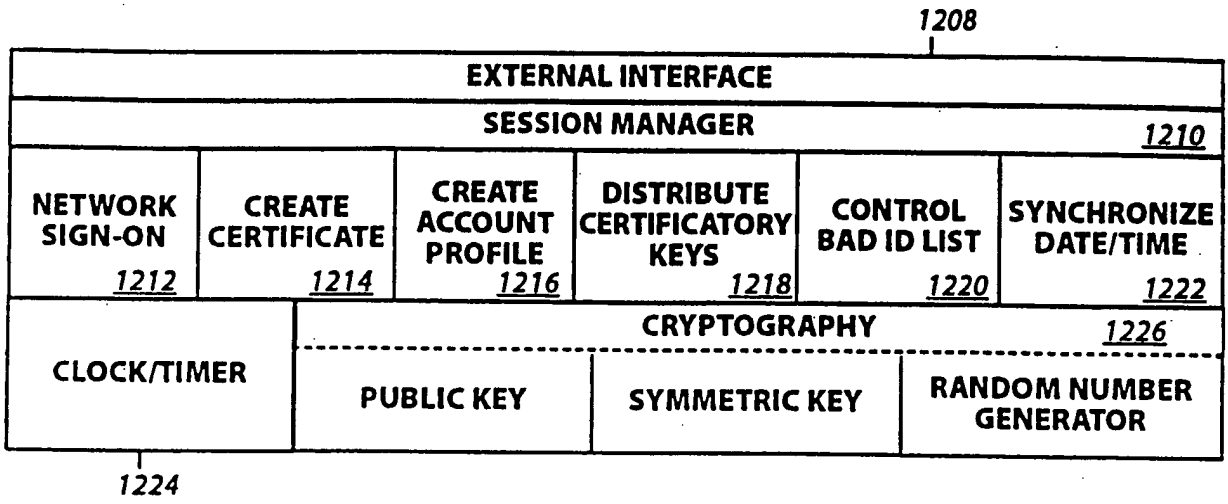

Figure 35A

Network Server

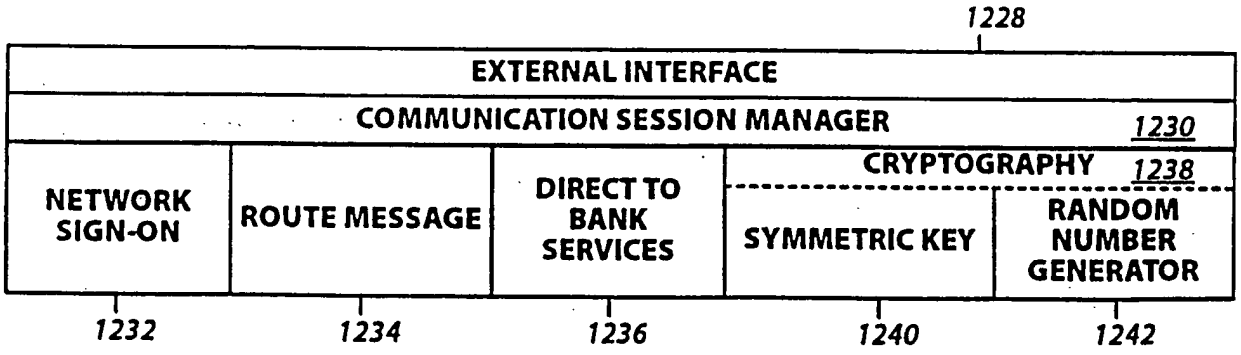

Figure 35B

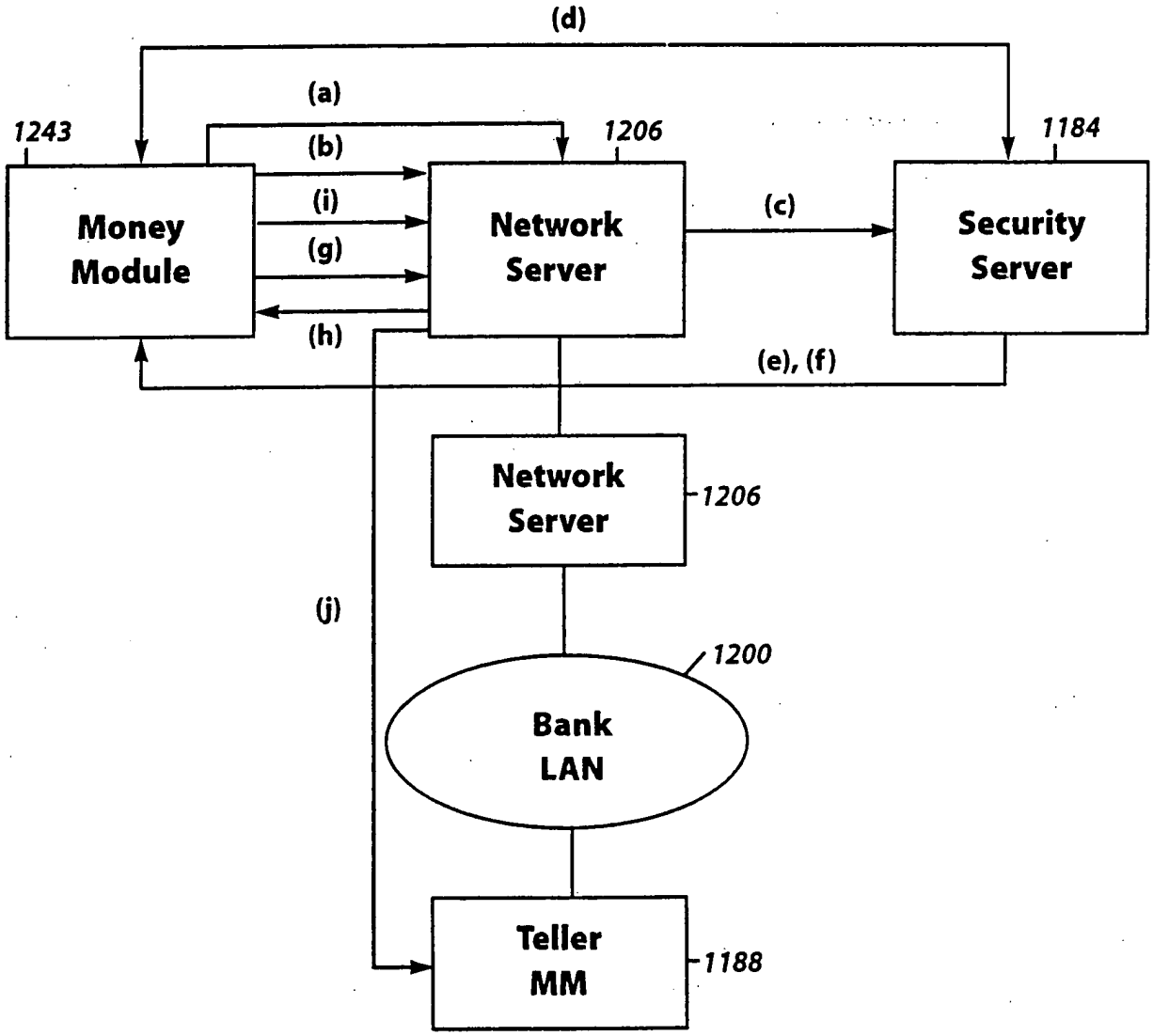
(d)
(a)
1243
(b)
1206
1184
Money Module
(i)
(g)
Network Server
(c)
Security Server
(h)
(e), (f)
Network Server
1206
(j)
1200
Bank LAN
Teller MM
1188

Figure 36

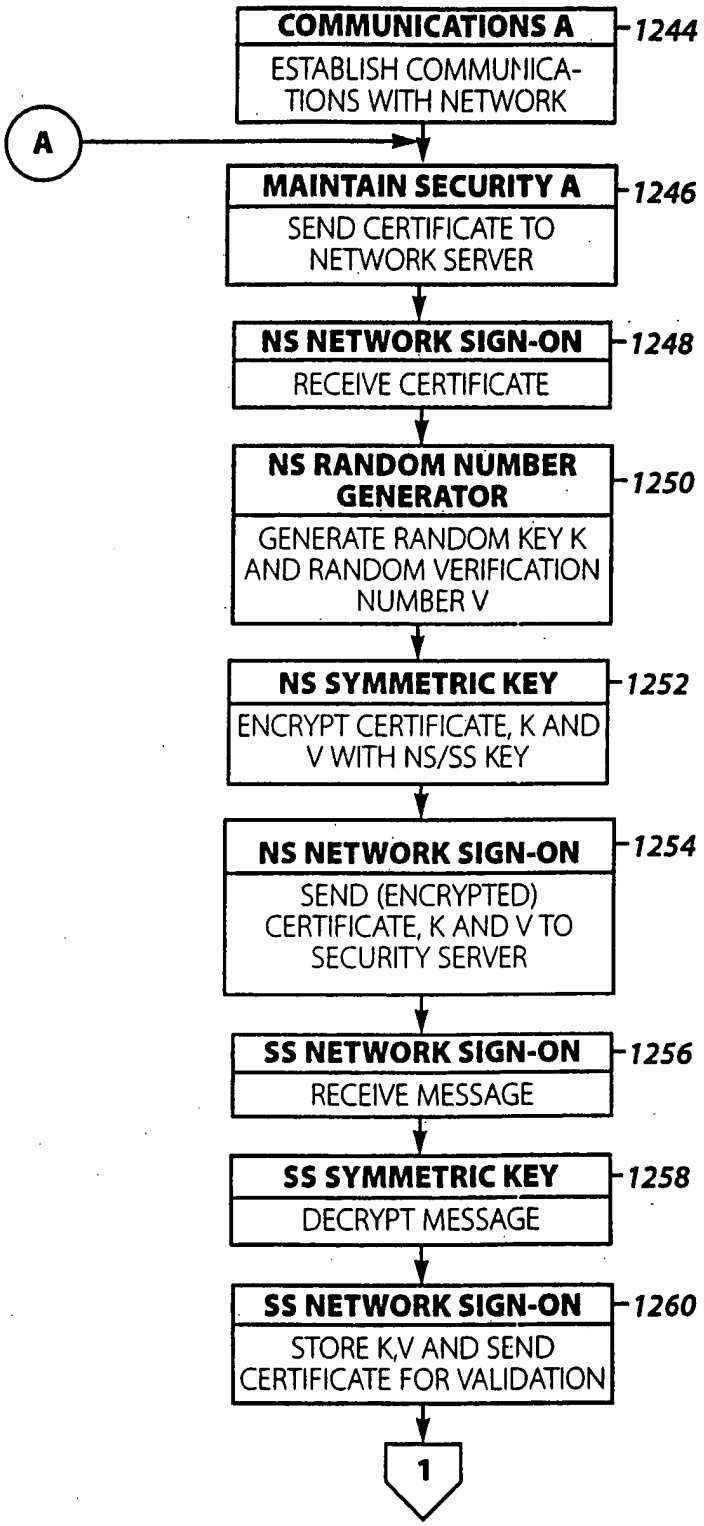
COMMUNICATIONS A
1244
ESTABLISH COMMUNICATIONS WITH NETWORK
A
MAINTAIN SECURITY A
1246
SEND CERTIFICATE TO NETWORK SERVER
NS NETWORK SIGN-ON
1248
RECEIVE CERTIFICATE
NS RANDOM NUMBER GENERATOR
1250
GENERATE RANDOM KEY K AND RANDOM VERIFICATION NUMBER V
NS SYMMETRIC KEY
1252
ENCRYPT CERTIFICATE, K AND V WITH NS/SS KEY
NS NETWORK SIGN-ON
1254
SEND (ENCRYPTED) CERTIFICATE, K AND V TO SECURITY SERVER
SS NETWORK SIGN-ON
1256
RECEIVE MESSAGE
SS SYMMETRIC KEY
1258
DECRYPT MESSAGE
SS NETWORK SIGN-ON
1260
STORE K,V AND SEND CERTIFICATE FOR VALIDATION
1

Figure 37A

63/91

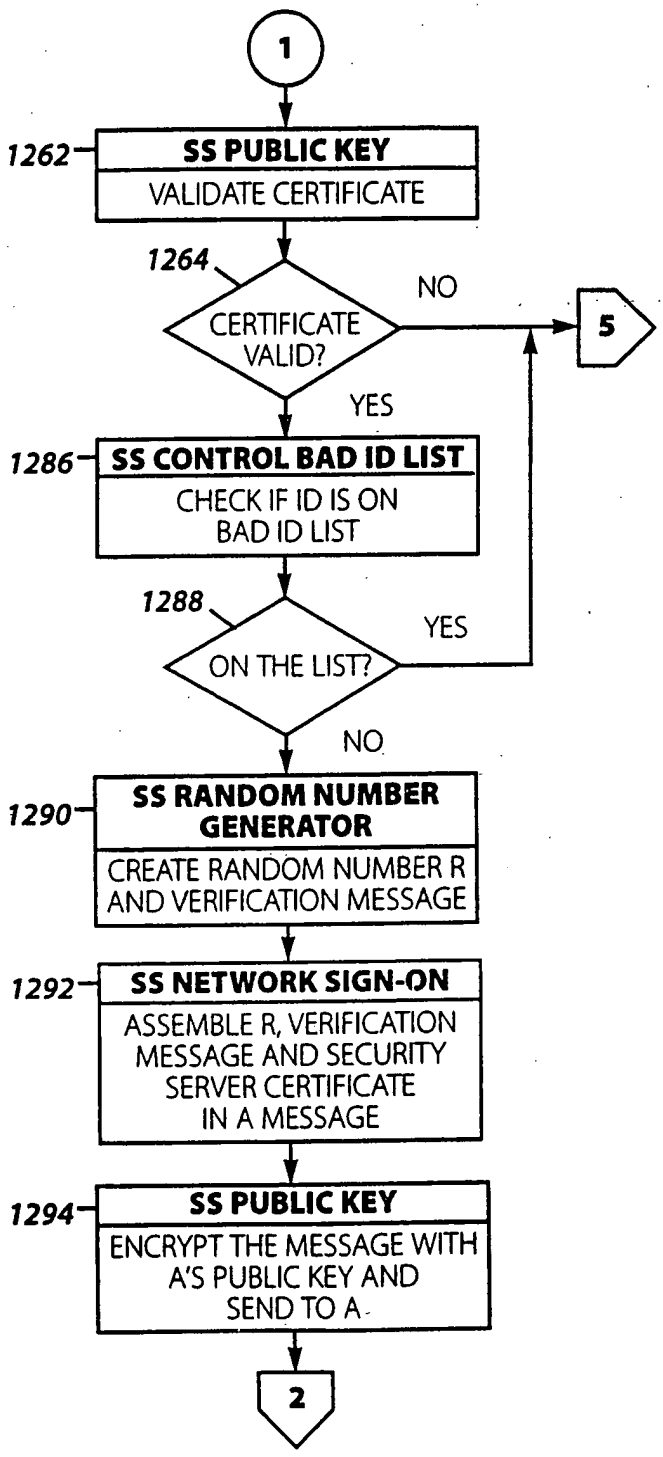

Figure 37B

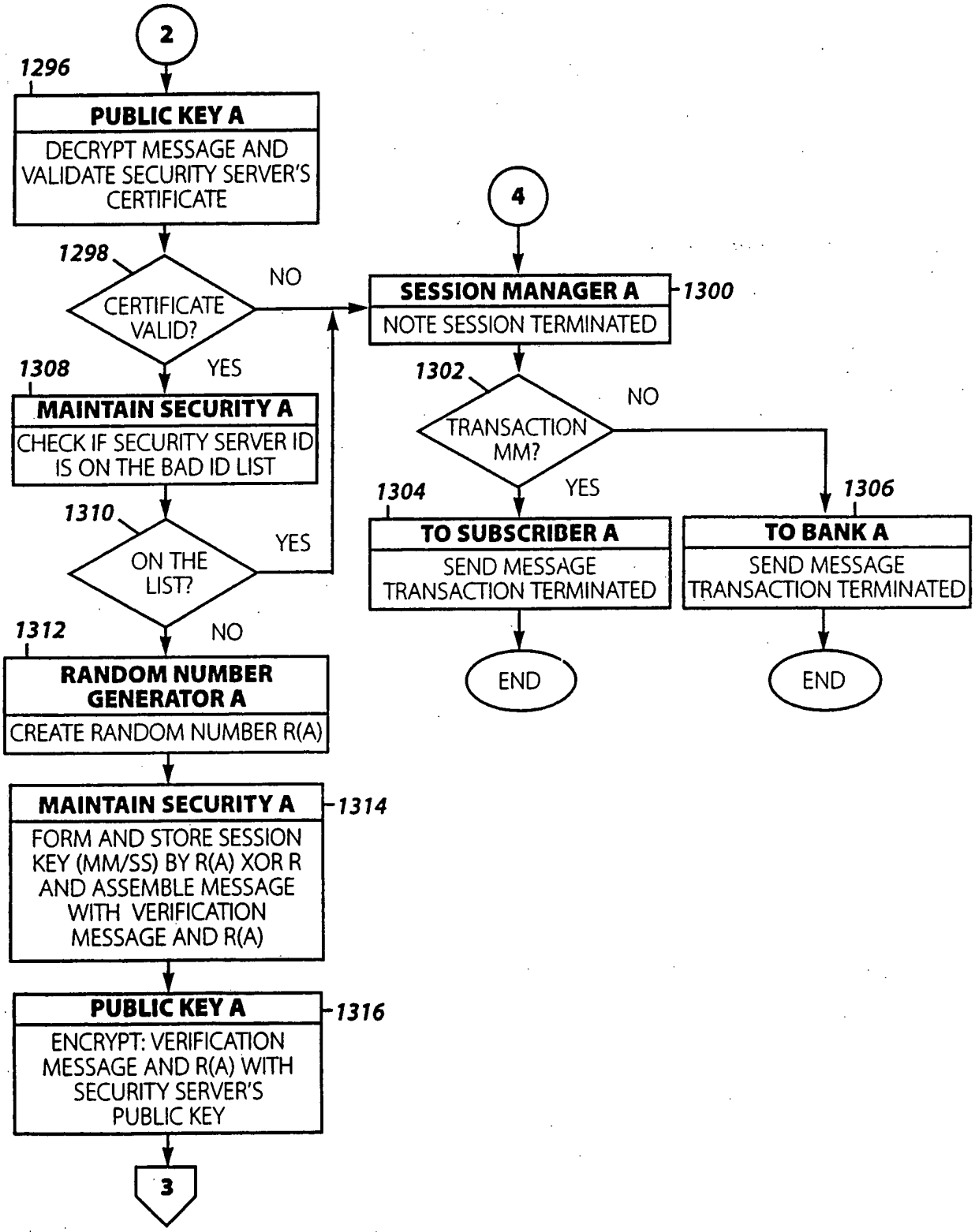
2
1296
PUBLIC KEY A
DECRYPT MESSAGE AND VALIDATE SECURITY SERVER'S CERTIFICATE
1298
CERTIFICATE VALID?
NO
YES
1308
MAINTAIN SECURITY A
CHECK IF SECURITY SERVER ID IS ON THE BAD ID LIST
1310
ON THE LIST?
YES
NO
1312
RANDOM NUMBER GENERATOR A
CREATE RANDOM NUMBER R(A)
MAINTAIN SECURITY A
1314
FORM AND STORE SESSION KEY (MM/SS) BY R(A) XOR R AND ASSEMBLE MESSAGE WITH VERIFICATION MESSAGE AND R(A)
PUBLIC KEY A
1316
ENCRYPT: VERIFICATION MESSAGE AND R(A) WITH SECURITY SERVER'S PUBLIC KEY
3
4
SESSION MANAGER A
1300
NOTE SESSION TERMINATED
1302
TRANSACTION MM?
NO
YES
1304
TO SUBSCRIBER A
SEND MESSAGE TRANSACTION TERMINATED
END
1306
TO BANK A
SEND MESSAGE TRANSACTION TERMINATED
END

Figure 37C

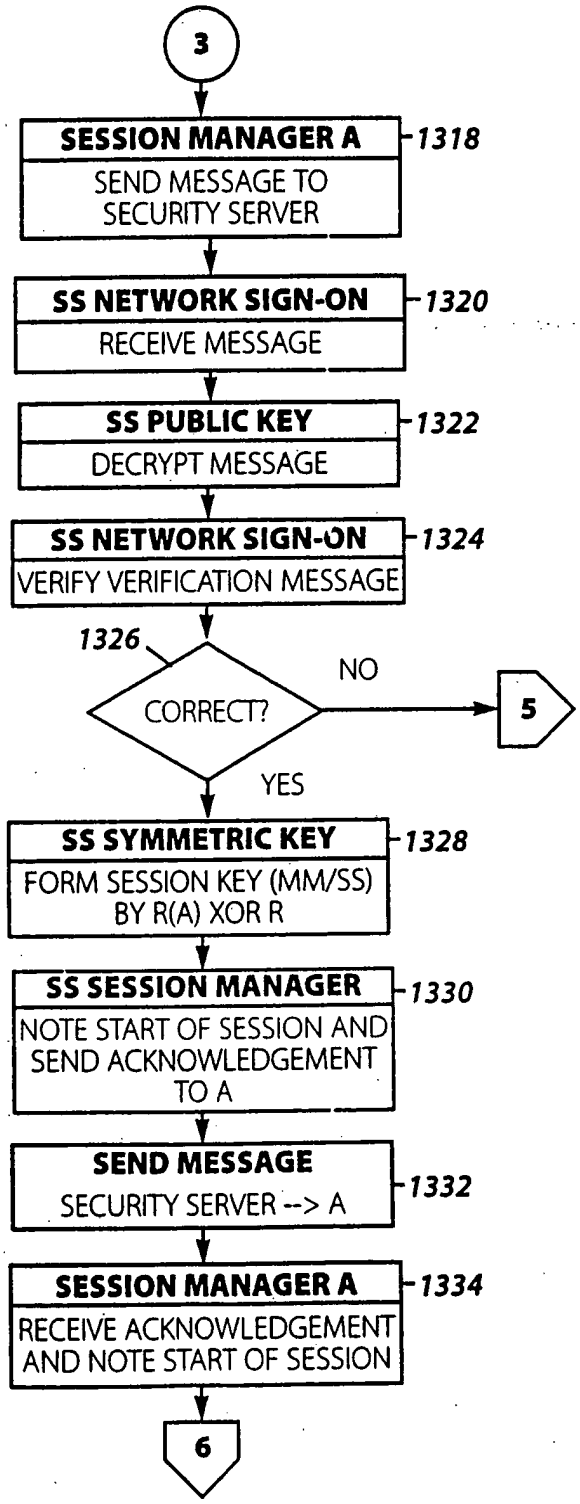
3
SESSION MANAGER A
SEND MESSAGE TO SECURITY SERVER
1318
SS NETWORK SIGN-ON
RECEIVE MESSAGE
1320
SS PUBLIC KEY
DECRYPT MESSAGE
1322
SS NETWORK SIGN-ON
VERIFY VERIFICATION MESSAGE
1324
1326
CORRECT?
NO
5
YES
SS SYMMETRIC KEY
FORM SESSION KEY (MM/SS) BY R(A) XOR R
1328
SS SESSION MANAGER
NOTE START OF SESSION AND SEND ACKNOWLEDGEMENT TO A
1330
SEND MESSAGE
SECURITY SERVER --> A
1332
SESSION MANAGER A
RECEIVE ACKNOWLEDGEMENT AND NOTE START OF SESSION
1334
6

Figure 37D

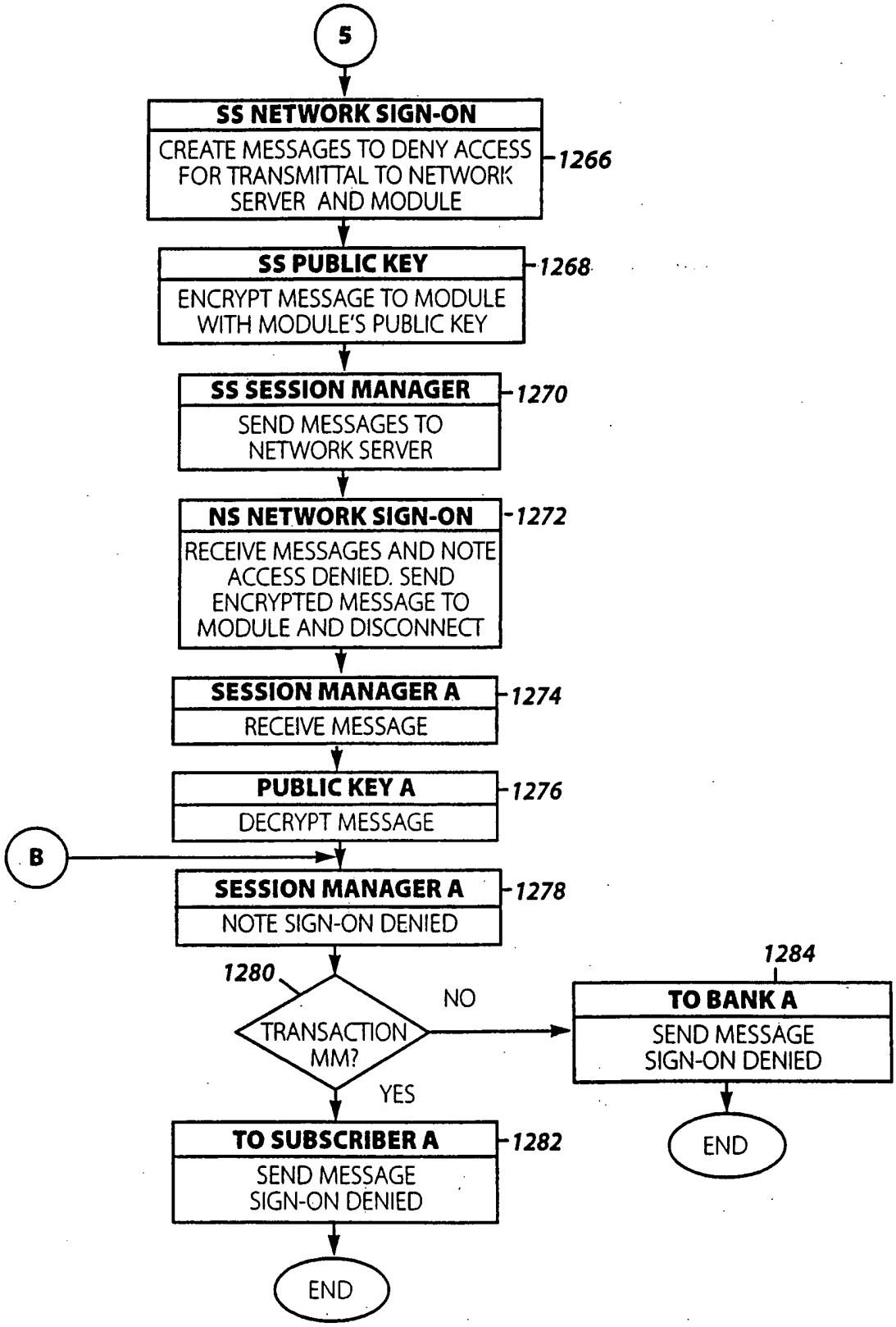
5
SS NETWORK SIGN-ON
CREATE MESSAGES TO DENY ACCESS FOR TRANSMITTAL TO NETWORK SERVER AND MODULE
1266
SS PUBLIC KEY
ENCRYPT MESSAGE TO MODULE WITH MODULE'S PUBLIC KEY
1268
SS SESSION MANAGER
SEND MESSAGES TO NETWORK SERVER
1270
NS NETWORK SIGN-ON
RECEIVE MESSAGES AND NOTE ACCESS DENIED. SEND ENCRYPTED MESSAGE TO MODULE AND DISCONNECT
1272
SESSION MANAGER A
RECEIVE MESSAGE
1274
PUBLIC KEY A
DECRYPT MESSAGE
1276
B
SESSION MANAGER A
NOTE SIGN-ON DENIED
1278
1280
TRANSACTION MM?
NO
YES
1284
TO BANK A
SEND MESSAGE SIGN-ON DENIED
END
TO SUBSCRIBER A
SEND MESSAGE SIGN-ON DENIED
1282
END

Figure 37E

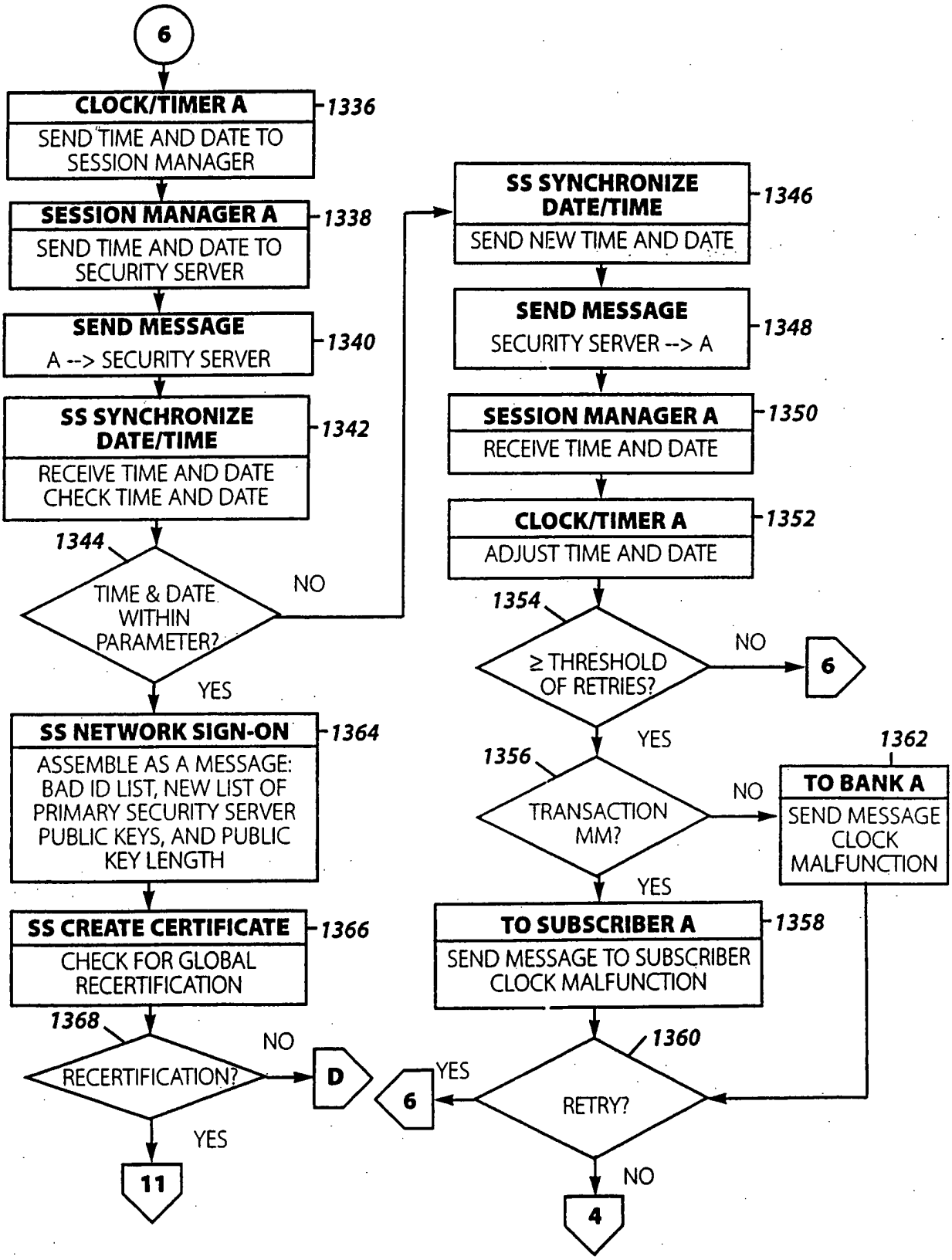
6
CLOCK/TIMER A
SEND TIME AND DATE TO SESSION MANAGER
1336
SESSION MANAGER A
SEND TIME AND DATE TO SECURITY SERVER
1338
SEND MESSAGE
A --> SECURITY SERVER
1340
SS SYNCHRONIZE DATE/TIME
RECEIVE TIME AND DATE CHECK TIME AND DATE
1342
1344
TIME & DATE WITHIN PARAMETER?
NO
YES
SS NETWORK SIGN-ON
ASSEMBLE AS A MESSAGE: BAD ID LIST, NEW LIST OF PRIMARY SECURITY SERVER PUBLIC KEYS, AND PUBLIC KEY LENGTH
1364
SS CREATE CERTIFICATE
CHECK FOR GLOBAL RECERTIFICATION
1366
1368
RECERTIFICATION?
NO
D
YES
11
SS SYNCHRONIZE DATE/TIME
SEND NEW TIME AND DATE
1346
SEND MESSAGE
SECURITY SERVER --> A
1348
SESSION MANAGER A
RECEIVE TIME AND DATE
1350
CLOCK/TIMER A
ADJUST TIME AND DATE
1352
1354
≥ THRESHOLD OF RETRIES?
NO
6
YES
1356
TRANSACTION MM?
NO
1362
TO BANK A
SEND MESSAGE CLOCK MALFUNCTION
YES
TO SUBSCRIBER A
SEND MESSAGE TO SUBSCRIBER CLOCK MALFUNCTION
1358
1360
RETRY?
YES
6
NO
4

Figure 37F

68/91

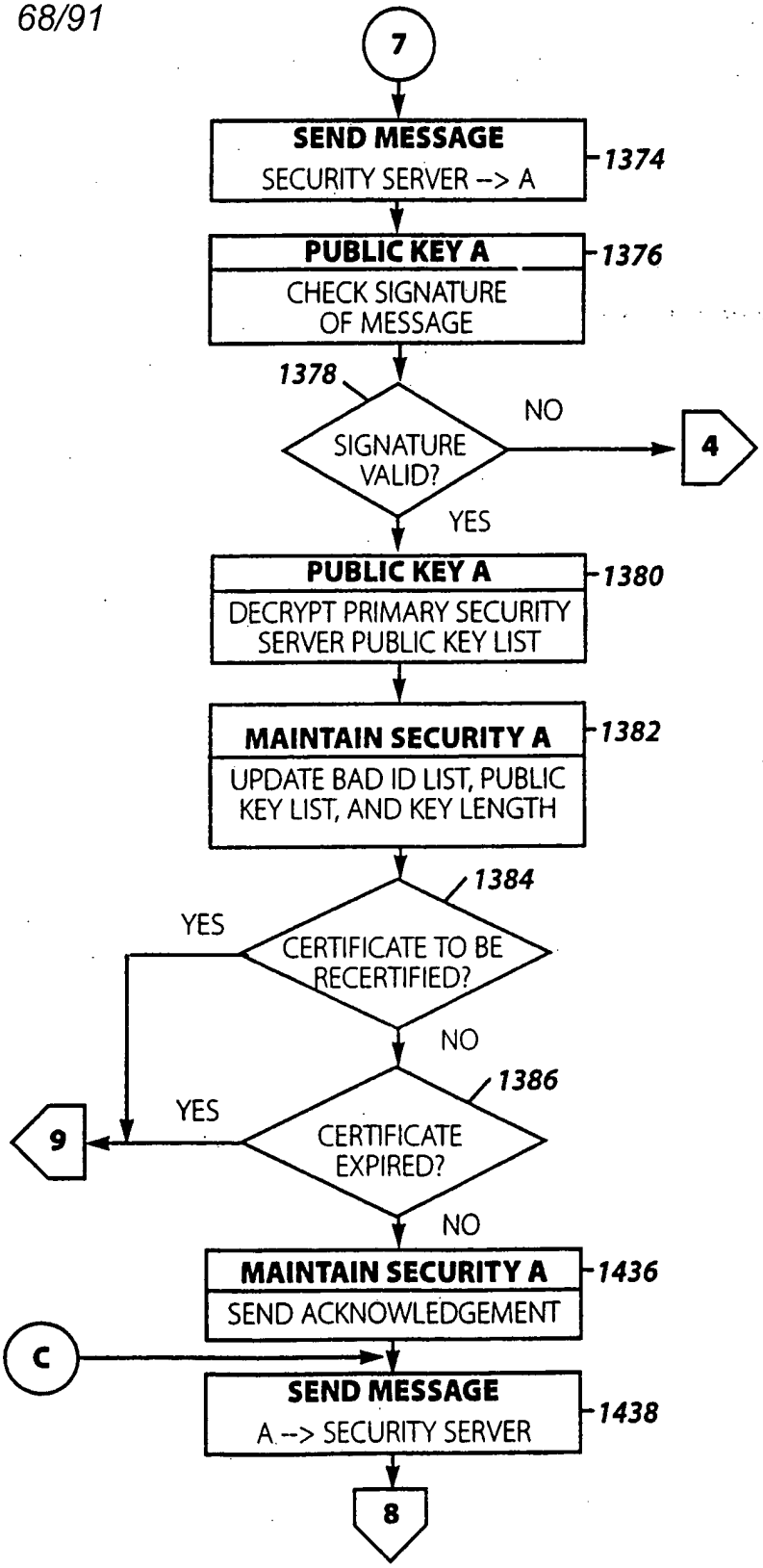

Figure 37G

69/91

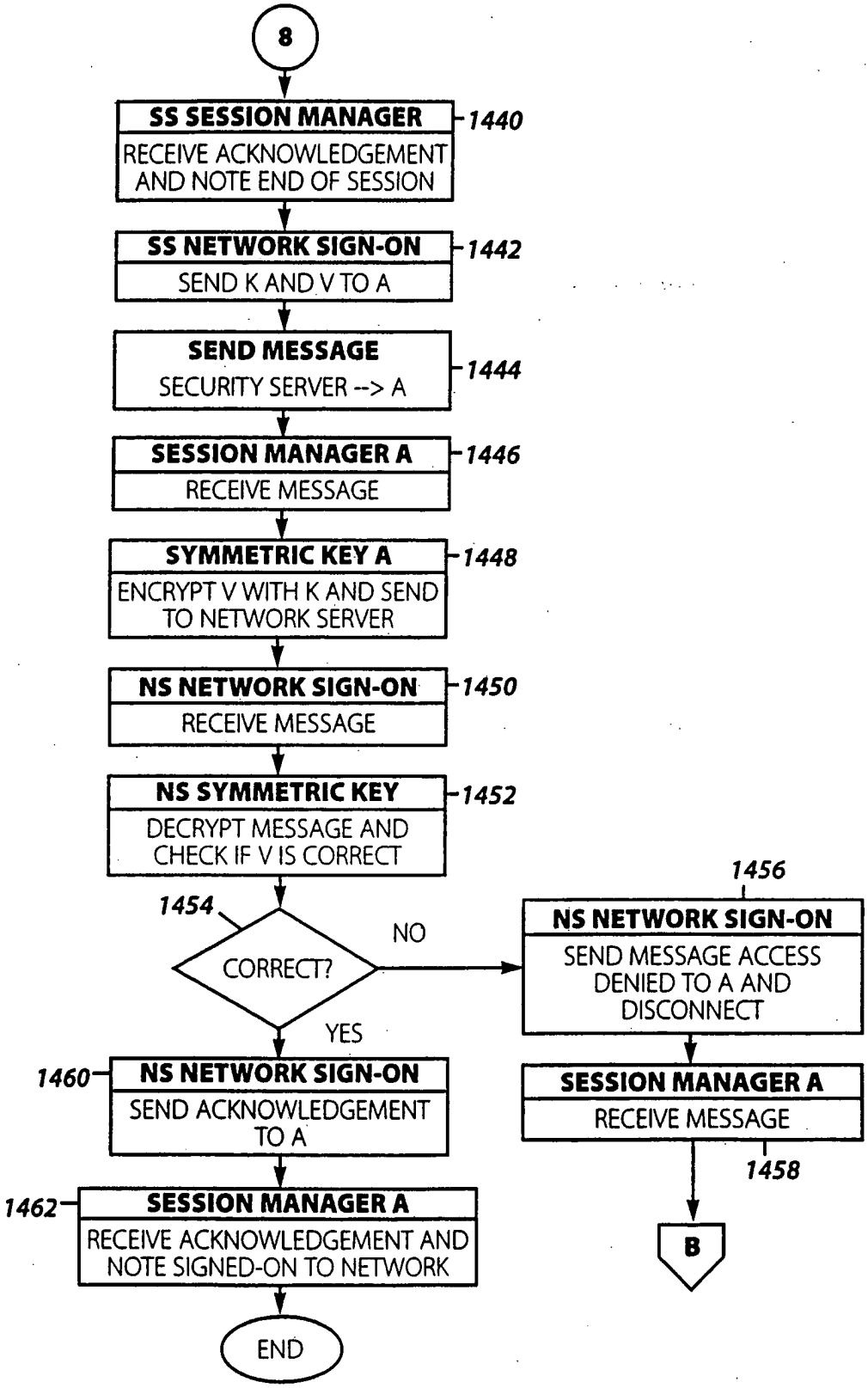

Figure 37H

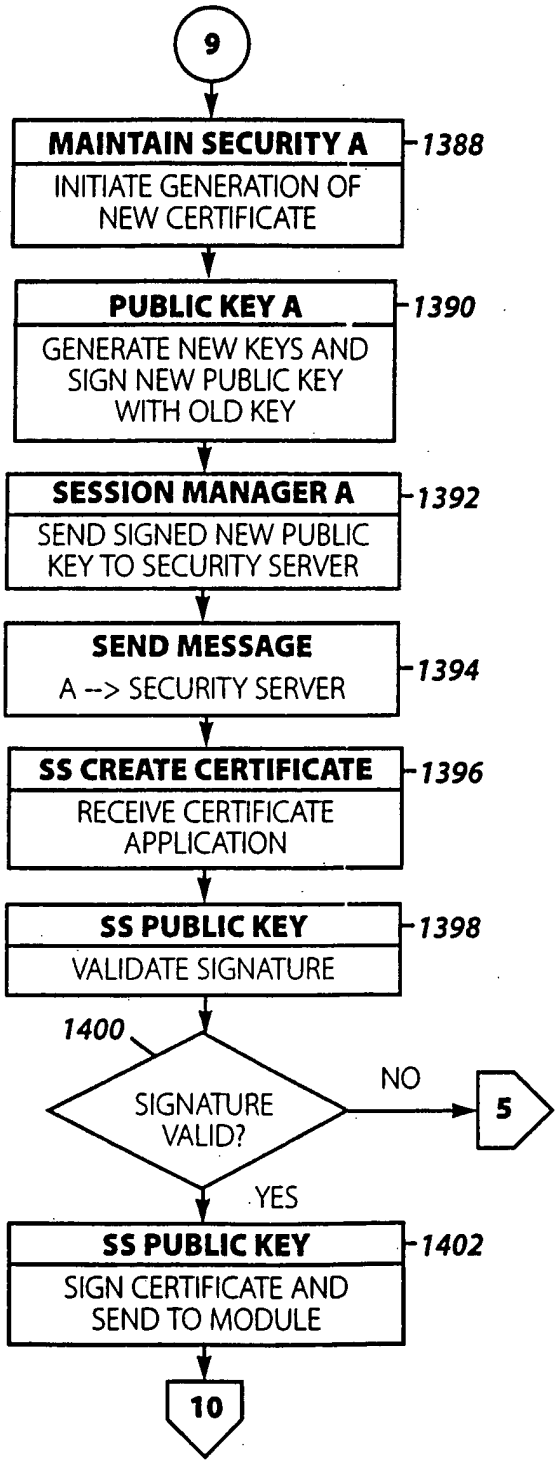
9
MAINTAIN SECURITY A
INITIATE GENERATION OF NEW CERTIFICATE
1388
PUBLIC KEY A
GENERATE NEW KEYS AND SIGN NEW PUBLIC KEY WITH OLD KEY
1390
SESSION MANAGER A
SEND SIGNED NEW PUBLIC KEY TO SECURITY SERVER
1392
SEND MESSAGE
A --> SECURITY SERVER
1394
SS CREATE CERTIFICATE
RECEIVE CERTIFICATE APPLICATION
1396
SS PUBLIC KEY
VALIDATE SIGNATURE
1398
1400
SIGNATURE VALID?
NO
5
YES
SS PUBLIC KEY
SIGN CERTIFICATE AND SEND TO MODULE
1402
10

Figure 37I

71/91

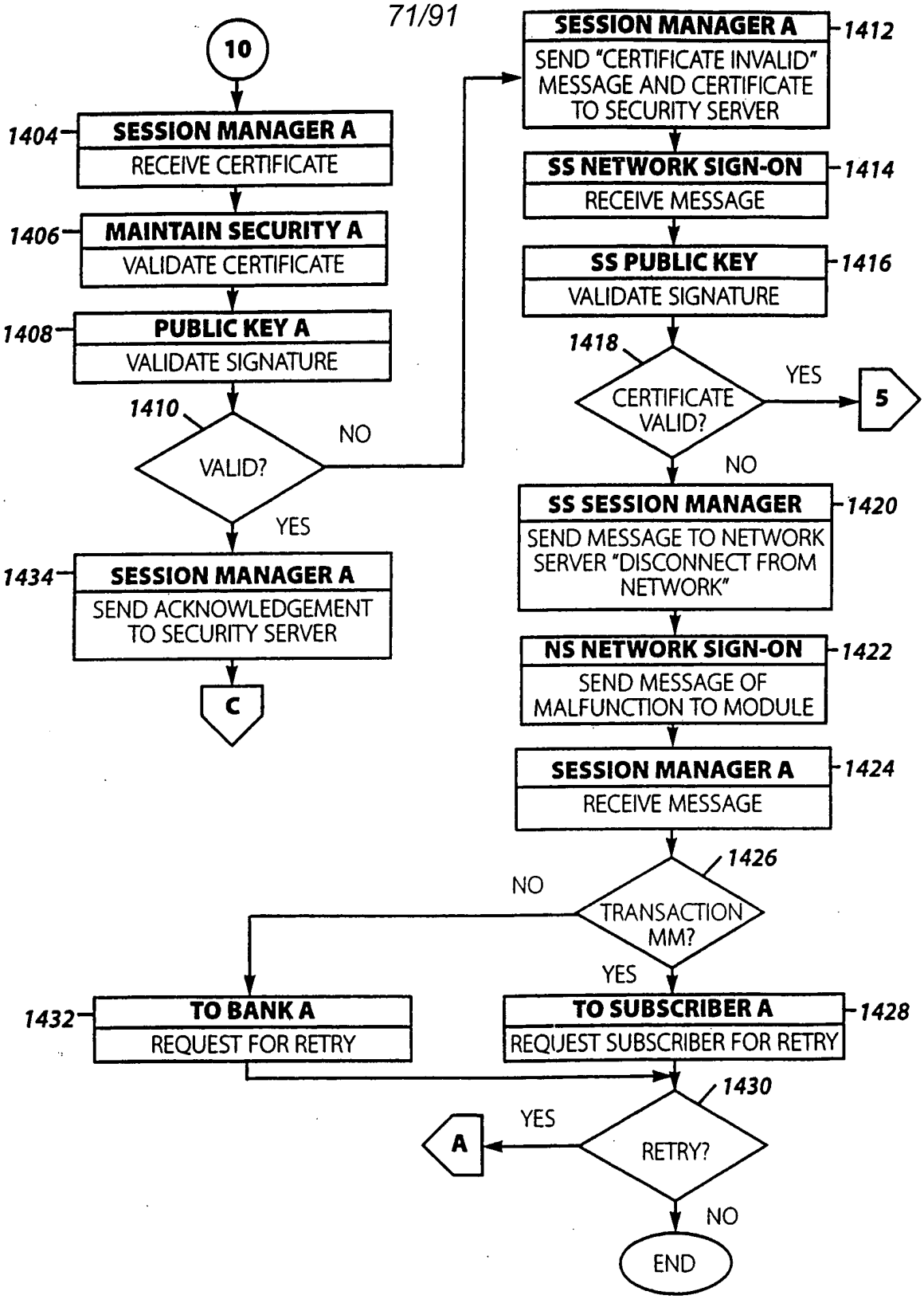

Figure 37J

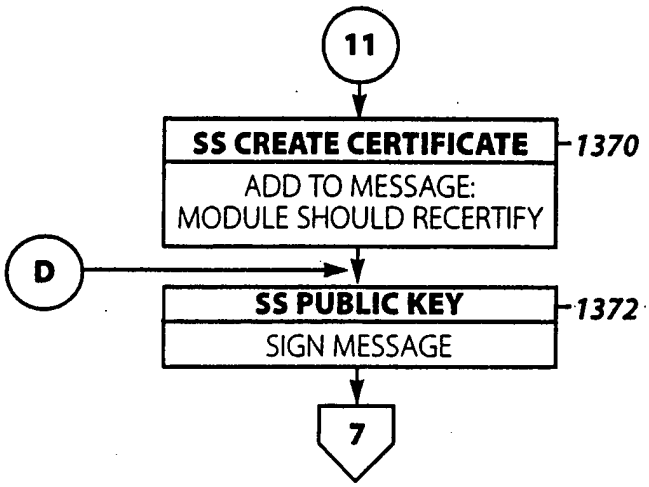
11
SS CREATE CERTIFICATE
1370
ADD TO MESSAGE:
MODULE SHOULD RECERTIFY
D
SS PUBLIC KEY
1372
SIGN MESSAGE
7

Figure 37K

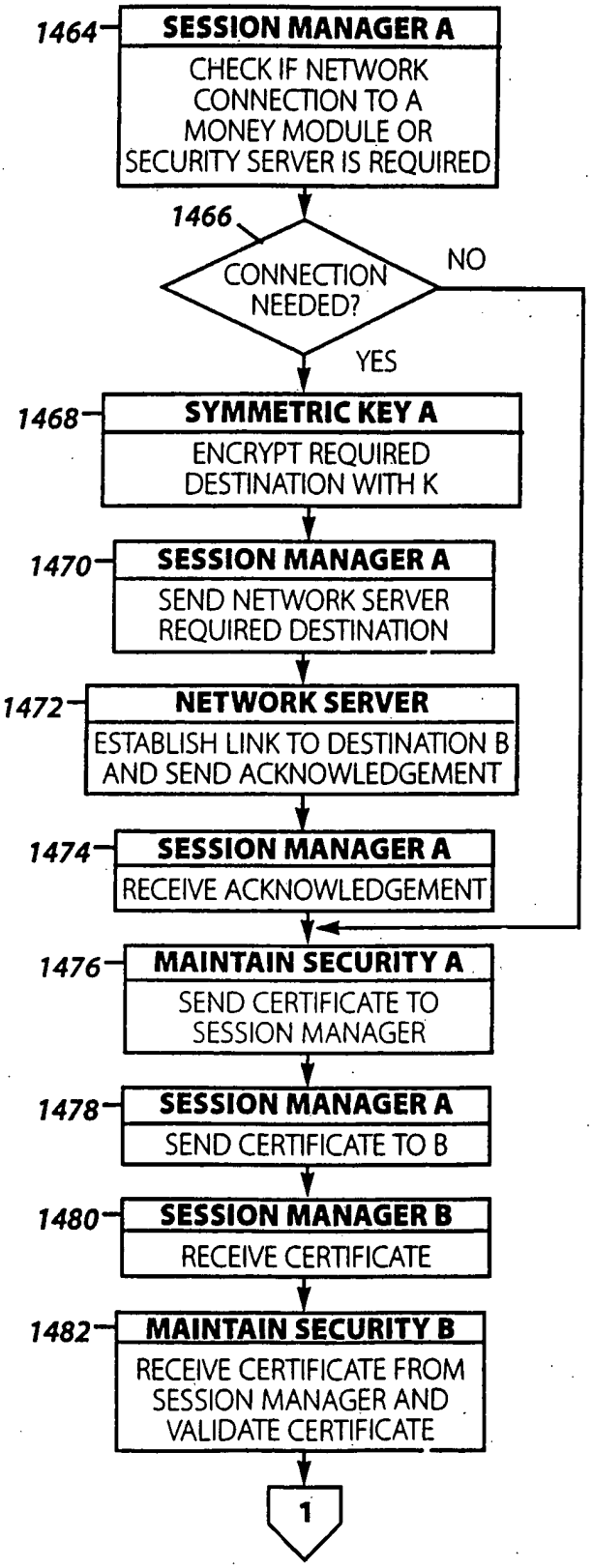
1464
SESSION MANAGER A
CHECK IF NETWORK CONNECTION TO A MONEY MODULE OR SECURITY SERVER IS REQUIRED
1466
CONNECTION NEEDED?
NO
YES
1468
SYMMETRIC KEY A
ENCRYPT REQUIRED DESTINATION WITH K
1470
SESSION MANAGER A
SEND NETWORK SERVER REQUIRED DESTINATION
1472
NETWORK SERVER
ESTABLISH LINK TO DESTINATION B AND SEND ACKNOWLEDGEMENT
1474
SESSION MANAGER A
RECEIVE ACKNOWLEDGEMENT
1476
MAINTAIN SECURITY A
SEND CERTIFICATE TO SESSION MANAGER
1478
SESSION MANAGER A
SEND CERTIFICATE TO B
1480
SESSION MANAGER B
RECEIVE CERTIFICATE
1482
MAINTAIN SECURITY B
RECEIVE CERTIFICATE FROM SESSION MANAGER AND VALIDATE CERTIFICATE
1

Figure 38A

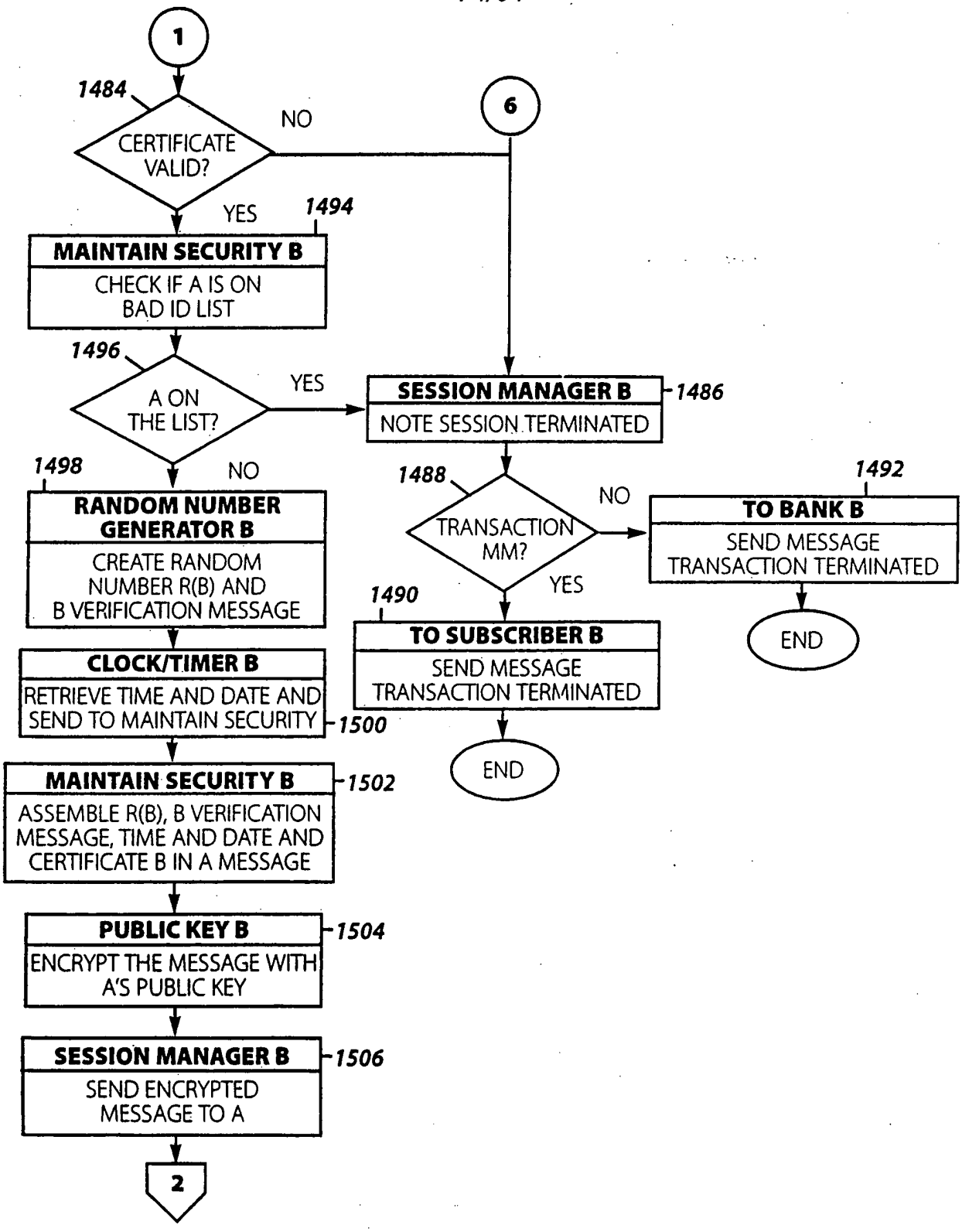
1
1484
CERTIFICATE VALID?
NO
6
YES
1494
MAINTAIN SECURITY B
CHECK IF A IS ON BAD ID LIST
1496
A ON THE LIST?
YES
SESSION MANAGER B
NOTE SESSION TERMINATED
1486
1498
NO
RANDOM NUMBER GENERATOR B
CREATE RANDOM NUMBER R(B) AND B VERIFICATION MESSAGE
1488
TRANSACTION MM?
NO
1492
TO BANK B
SEND MESSAGE TRANSACTION TERMINATED
YES
1490
TO SUBSCRIBER B
SEND MESSAGE TRANSACTION TERMINATED
END
END
CLOCK/TIMER B
RETRIEVE TIME AND DATE AND SEND TO MAINTAIN SECURITY
1500
MAINTAIN SECURITY B
1502
ASSEMBLE R(B), B VERIFICATION MESSAGE, TIME AND DATE AND CERTIFICATE B IN A MESSAGE
PUBLIC KEY B
1504
ENCRYPT THE MESSAGE WITH A'S PUBLIC KEY
SESSION MANAGER B
1506
SEND ENCRYPTED MESSAGE TO A
2

Figure 38B

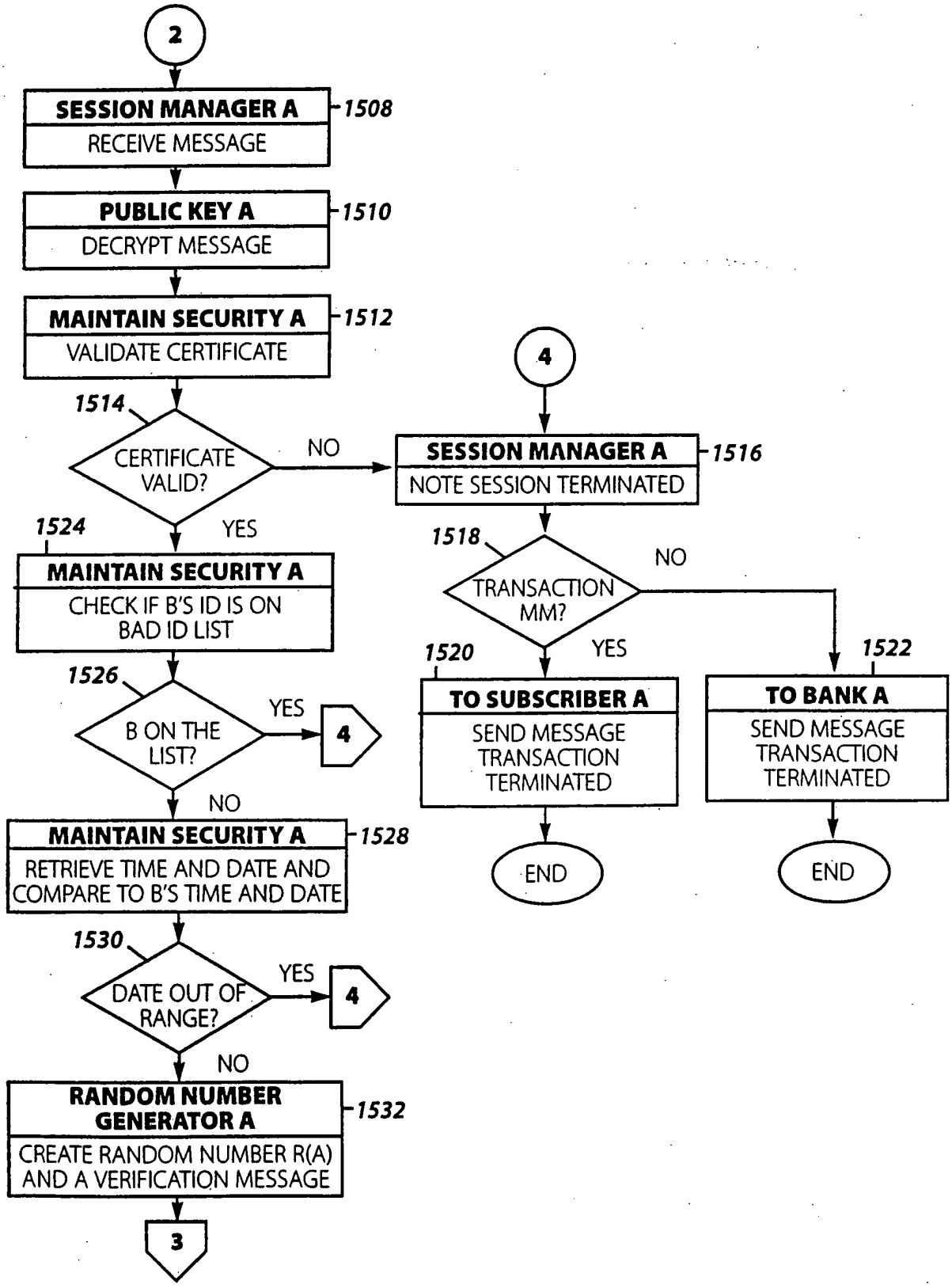
2
SESSION MANAGER A
RECEIVE MESSAGE
1508
PUBLIC KEY A
DECRYPT MESSAGE
1510
MAINTAIN SECURITY A
VALIDATE CERTIFICATE
1512
1514
CERTIFICATE VALID?
NO
YES
4
SESSION MANAGER A
NOTE SESSION TERMINATED
1516
1518
TRANSACTION MM?
NO
YES
1520
TO SUBSCRIBER A
SEND MESSAGE TRANSACTION TERMINATED
END
1522
TO BANK A
SEND MESSAGE TRANSACTION TERMINATED
END
1524
MAINTAIN SECURITY A
CHECK IF B'S ID IS ON BAD ID LIST
1526
B ON THE LIST?
YES
4
NO
MAINTAIN SECURITY A
RETRIEVE TIME AND DATE AND COMPARE TO B'S TIME AND DATE
1528
1530
DATE OUT OF RANGE?
YES
4
NO
RANDOM NUMBER GENERATOR A
CREATE RANDOM NUMBER R(A) AND A VERIFICATION MESSAGE
1532
3

Figure 38C

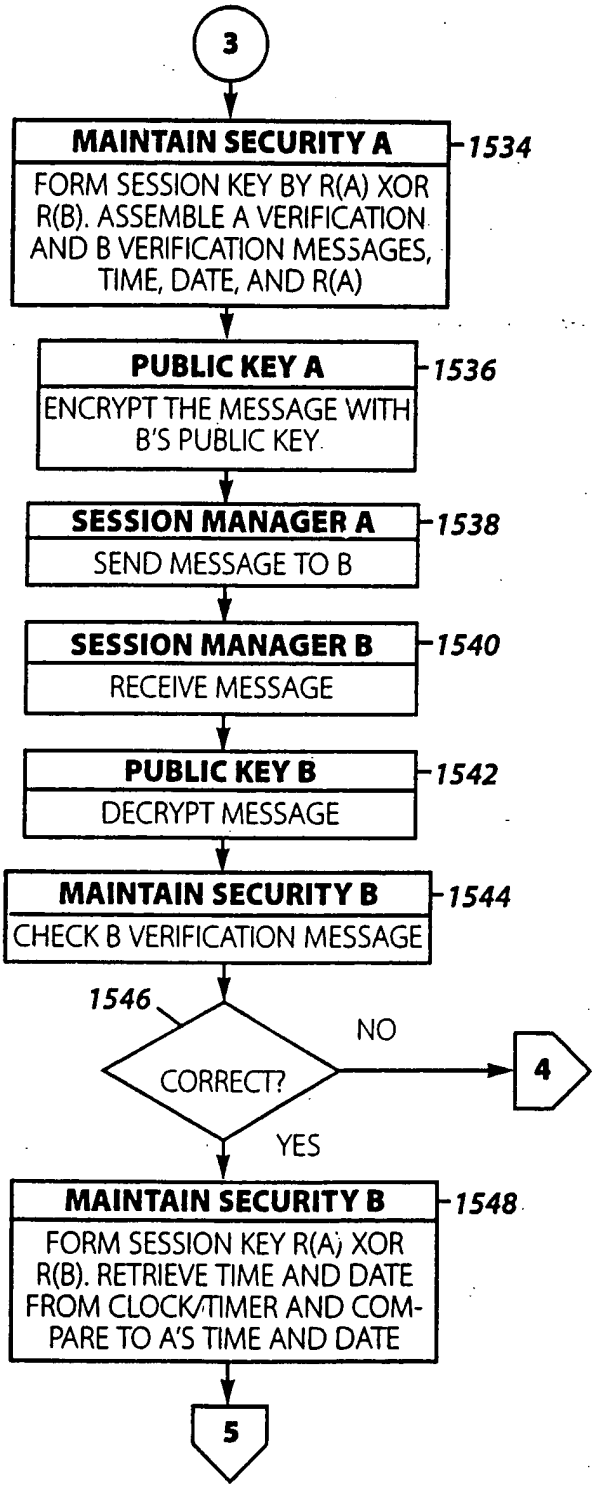
3
MAINTAIN SECURITY A
1534
FORM SESSION KEY BY R(A) XOR R(B). ASSEMBLE A VERIFICATION AND B VERIFICATION MESSAGES, TIME, DATE, AND R(A)
PUBLIC KEY A
1536
ENCRYPT THE MESSAGE WITH B'S PUBLIC KEY
SESSION MANAGER A
1538
SEND MESSAGE TO B
SESSION MANAGER B
1540
RECEIVE MESSAGE
PUBLIC KEY B
1542
DECRYPT MESSAGE
MAINTAIN SECURITY B
1544
CHECK B VERIFICATION MESSAGE
1546
CORRECT?
NO
4
YES
MAINTAIN SECURITY B
1548
FORM SESSION KEY R(A) XOR R(B). RETRIEVE TIME AND DATE FROM CLOCK/TIMER AND COMPARE TO A'S TIME AND DATE
5

Figure 38D

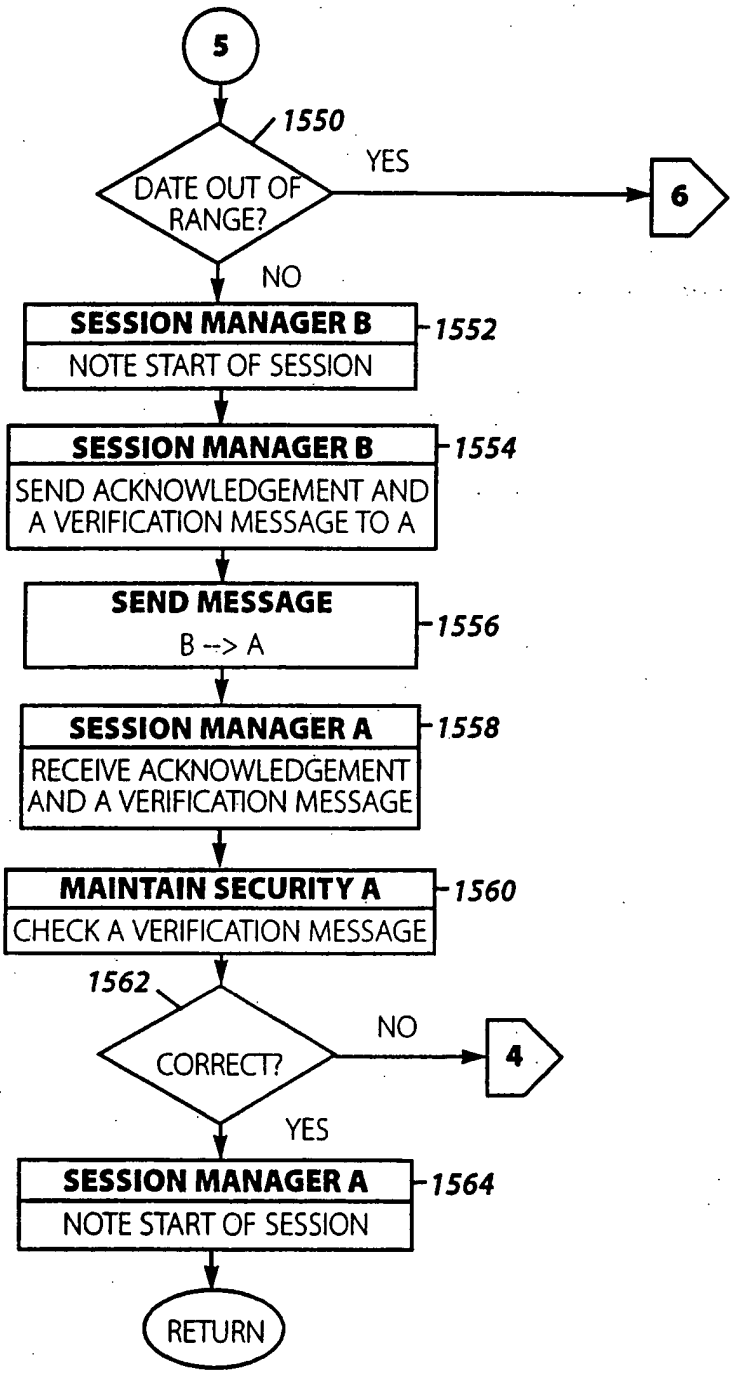
5
1550
DATE OUT OF RANGE?
YES
6
NO
SESSION MANAGER B
NOTE START OF SESSION
1552
SESSION MANAGER B
SEND ACKNOWLEDGEMENT AND A VERIFICATION MESSAGE TO A
1554
SEND MESSAGE
B --> A
1556
SESSION MANAGER A
RECEIVE ACKNOWLEDGEMENT AND A VERIFICATION MESSAGE
1558
MAINTAIN SECURITY A
CHECK A VERIFICATION MESSAGE
1560
1562
CORRECT?
NO
4
YES
SESSION MANAGER A
NOTE START OF SESSION
1564
RETURN

Figure 38E

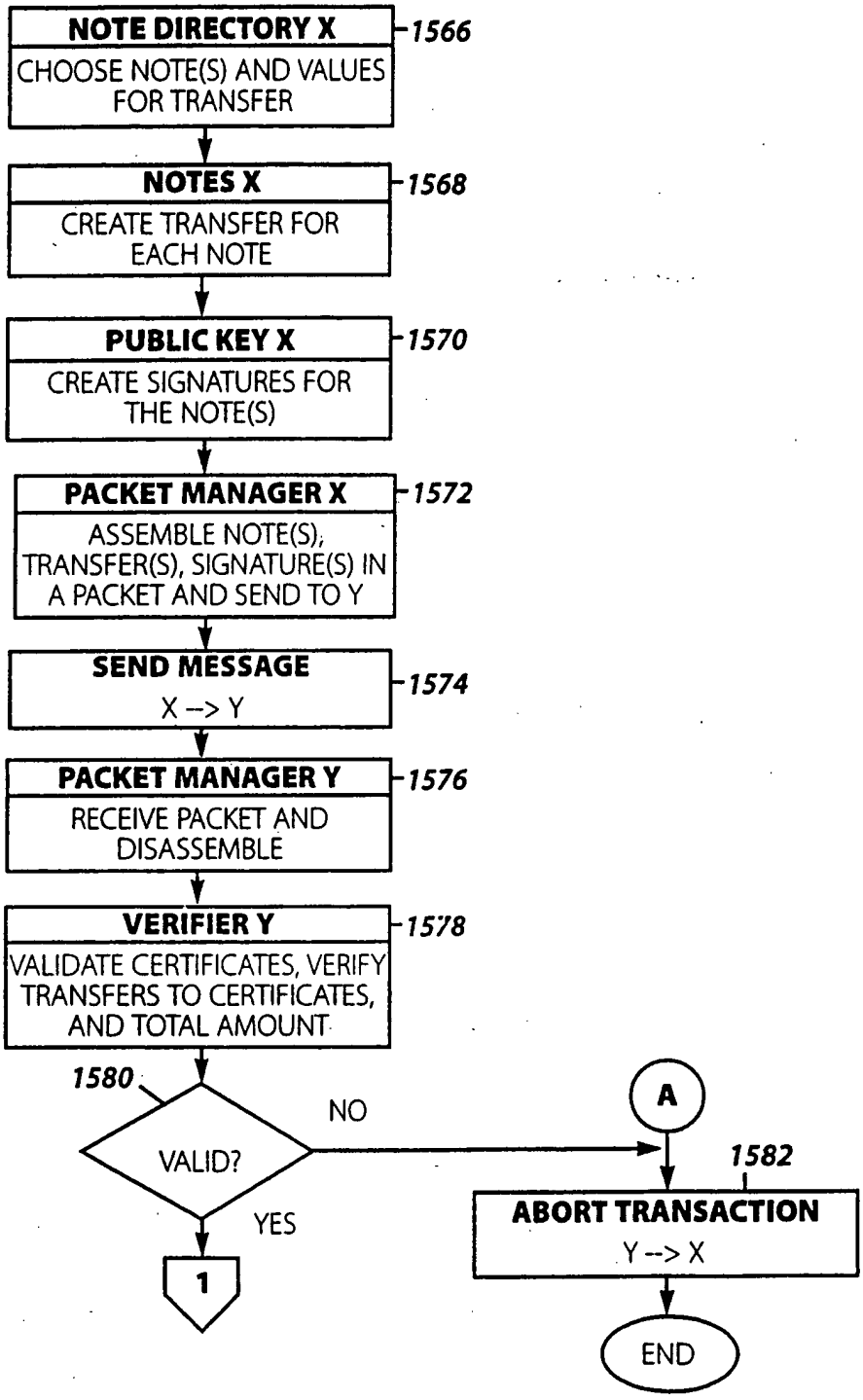
NOTE DIRECTORY X
1566
CHOOSE NOTE(S) AND VALUES FOR TRANSFER
NOTES X
1568
CREATE TRANSFER FOR EACH NOTE
PUBLIC KEY X
1570
CREATE SIGNATURES FOR THE NOTE(S)
PACKET MANAGER X
1572
ASSEMBLE NOTE(S), TRANSFER(S), SIGNATURE(S) IN A PACKET AND SEND TO Y
SEND MESSAGE
X --> Y
1574
PACKET MANAGER Y
1576
RECEIVE PACKET AND DISASSEMBLE
VERIFIER Y
1578
VALIDATE CERTIFICATES, VERIFY TRANSFERS TO CERTIFICATES, AND TOTAL AMOUNT
1580
VALID?
NO
YES
A
1582
ABORT TRANSACTION
Y --> X
1
END

Figure 39A

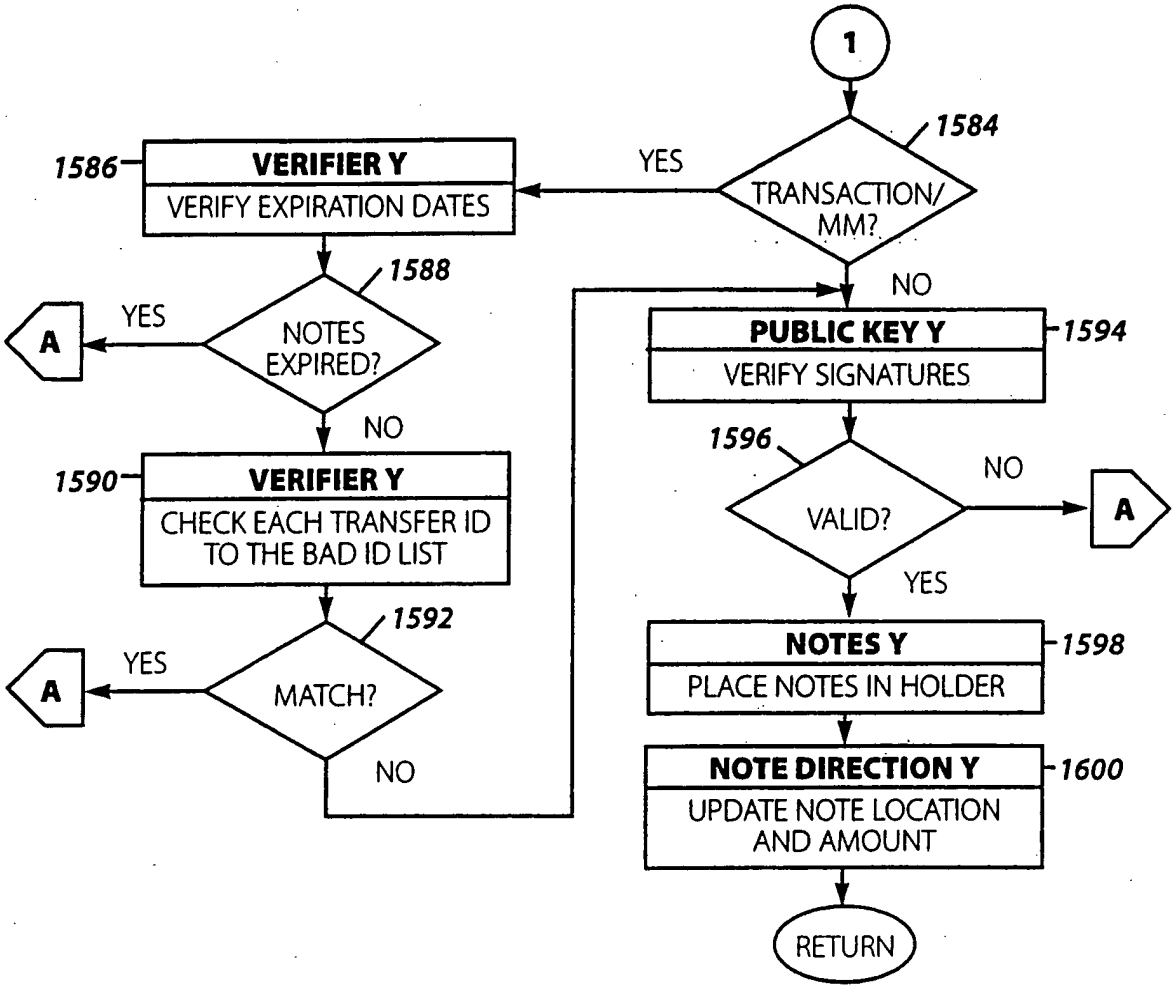
1
1584
TRANSACTION/ MM?
YES
1586
VERIFIER Y
VERIFY EXPIRATION DATES
NO
1588
NOTES EXPIRED?
YES
A
NO
PUBLIC KEY Y
VERIFY SIGNATURES
1594
1590
VERIFIER Y
CHECK EACH TRANSFER ID TO THE BAD ID LIST
1596
VALID?
NO
A
YES
1592
MATCH?
YES
A
NO
NOTES Y
PLACE NOTES IN HOLDER
1598
NOTE DIRECTION Y
UPDATE NOTE LOCATION AND AMOUNT
1600
RETURN

Figure 39B

80/91

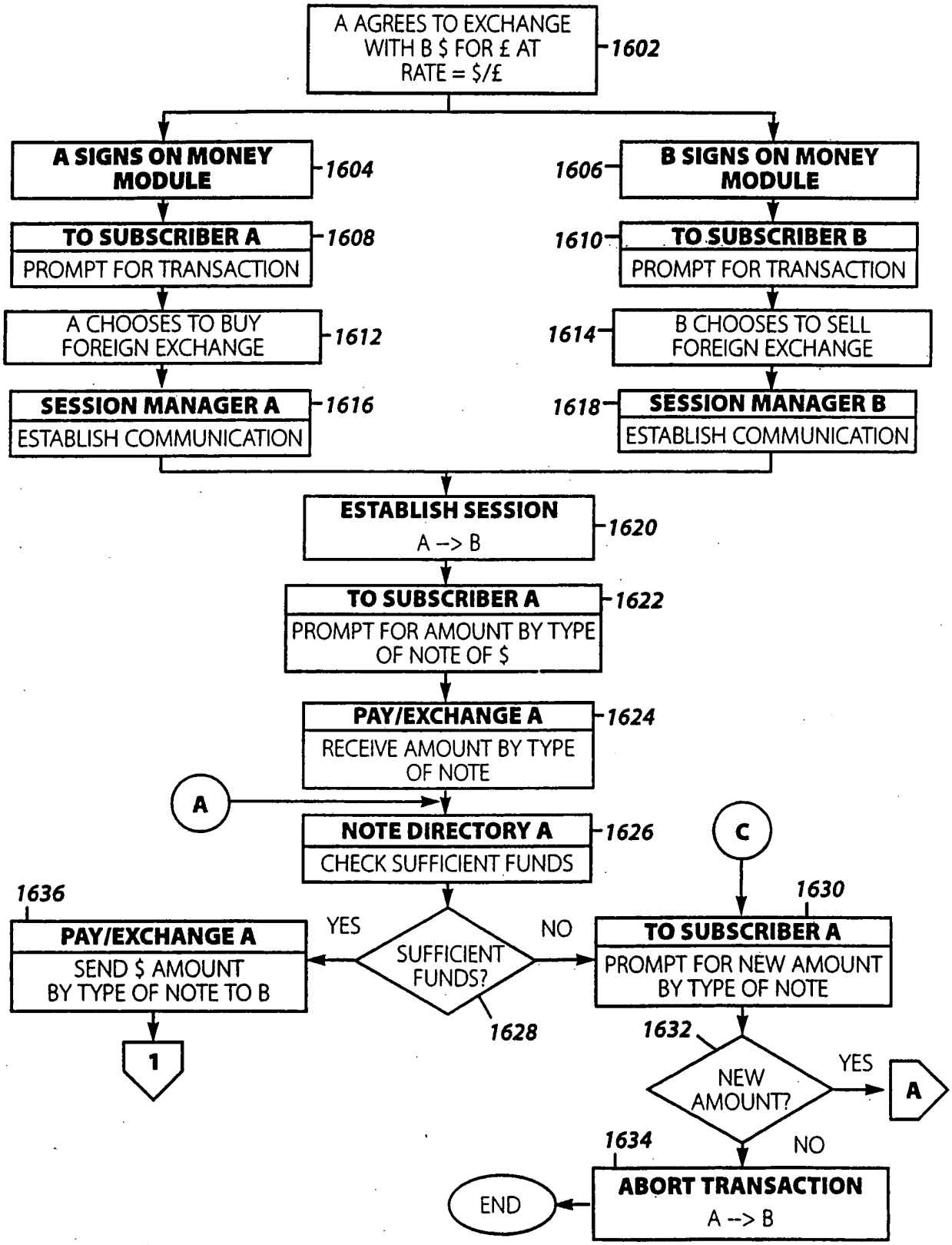

Figure 40A

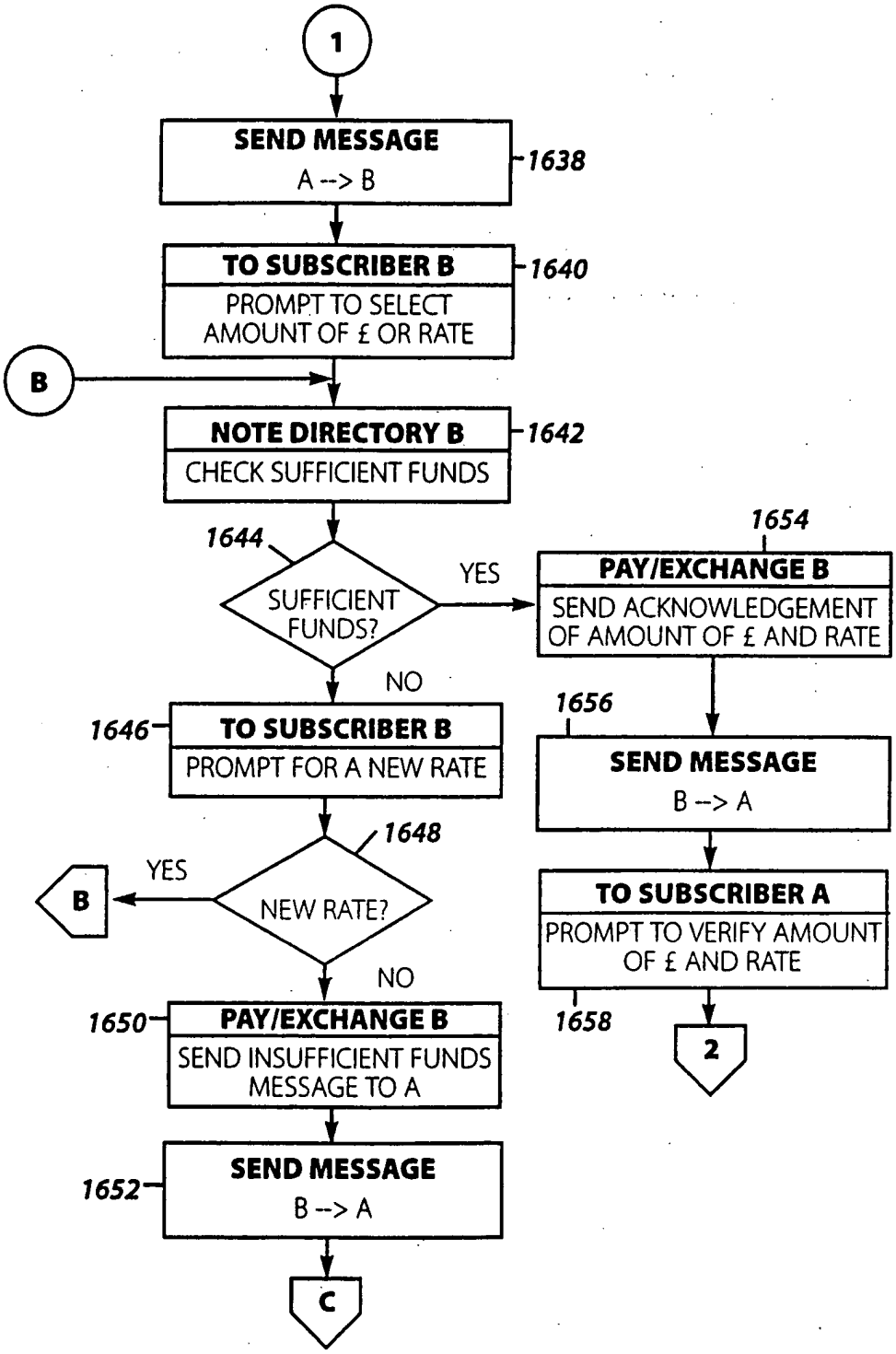
1
SEND MESSAGE
A --> B
1638
TO SUBSCRIBER B
PROMPT TO SELECT AMOUNT OF £ OR RATE
1640
B
NOTE DIRECTORY B
CHECK SUFFICIENT FUNDS
1642
1644
SUFFICIENT FUNDS?
YES
1654
PAY/EXCHANGE B
SEND ACKNOWLEDGEMENT OF AMOUNT OF £ AND RATE
NO
1646
TO SUBSCRIBER B
PROMPT FOR A NEW RATE
1656
SEND MESSAGE
B --> A
1648
B
YES
NEW RATE?
TO SUBSCRIBER A
PROMPT TO VERIFY AMOUNT OF £ AND RATE
NO
1650
PAY/EXCHANGE B
SEND INSUFFICIENT FUNDS MESSAGE TO A
1658
2
1652
SEND MESSAGE
B --> A
C

Figure 40B

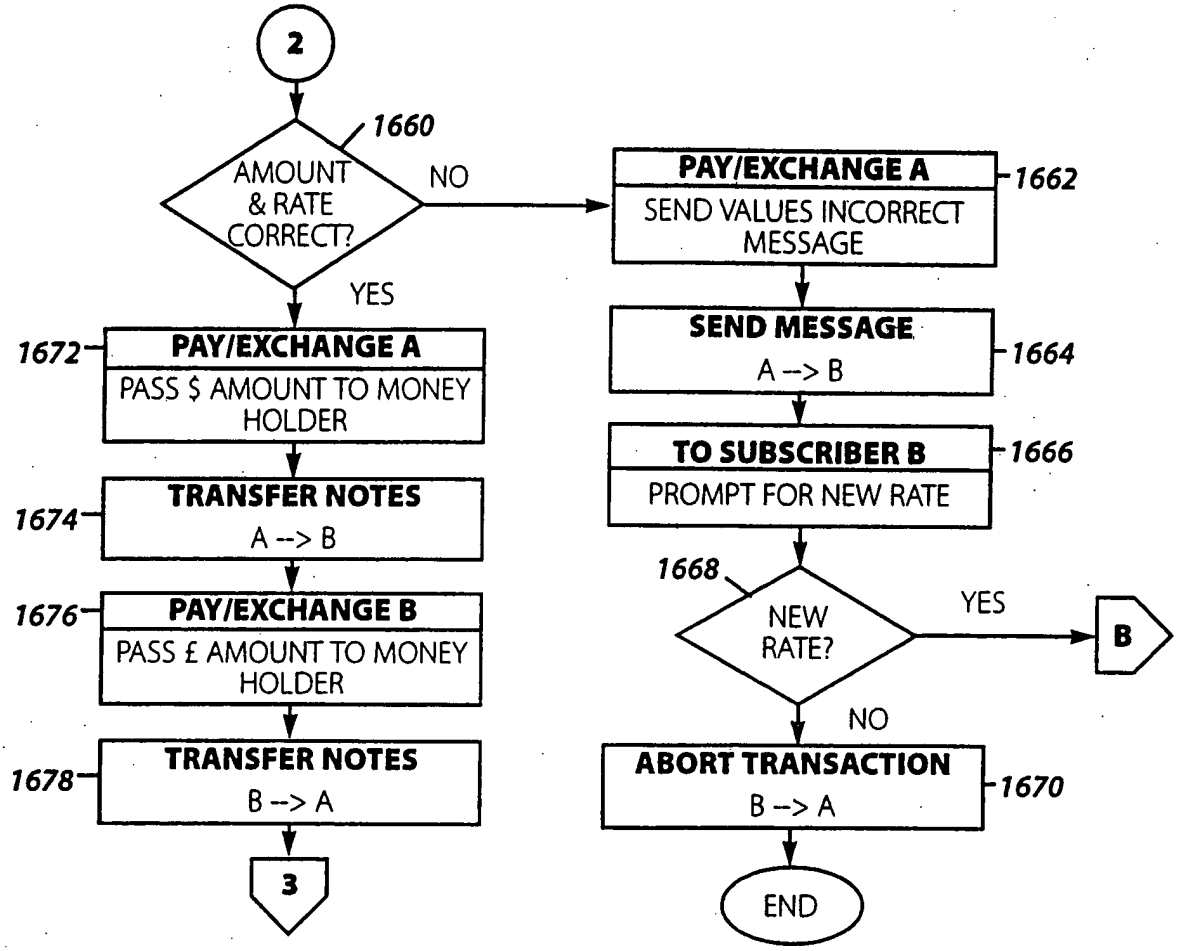
2
1660
AMOUNT & RATE CORRECT?
NO
YES
PAY/EXCHANGE A
SEND VALUES INCORRECT MESSAGE
1662
SEND MESSAGE
A --> B
1664
TO SUBSCRIBER B
PROMPT FOR NEW RATE
1666
1668
NEW RATE?
YES
B
NO
ABORT TRANSACTION
B --> A
1670
END
1672
PAY/EXCHANGE A
PASS $ AMOUNT TO MONEY HOLDER
1674
TRANSFER NOTES
A --> B
1676
PAY/EXCHANGE B
PASS £ AMOUNT TO MONEY HOLDER
1678
TRANSFER NOTES
B --> A
3

Figure 40C

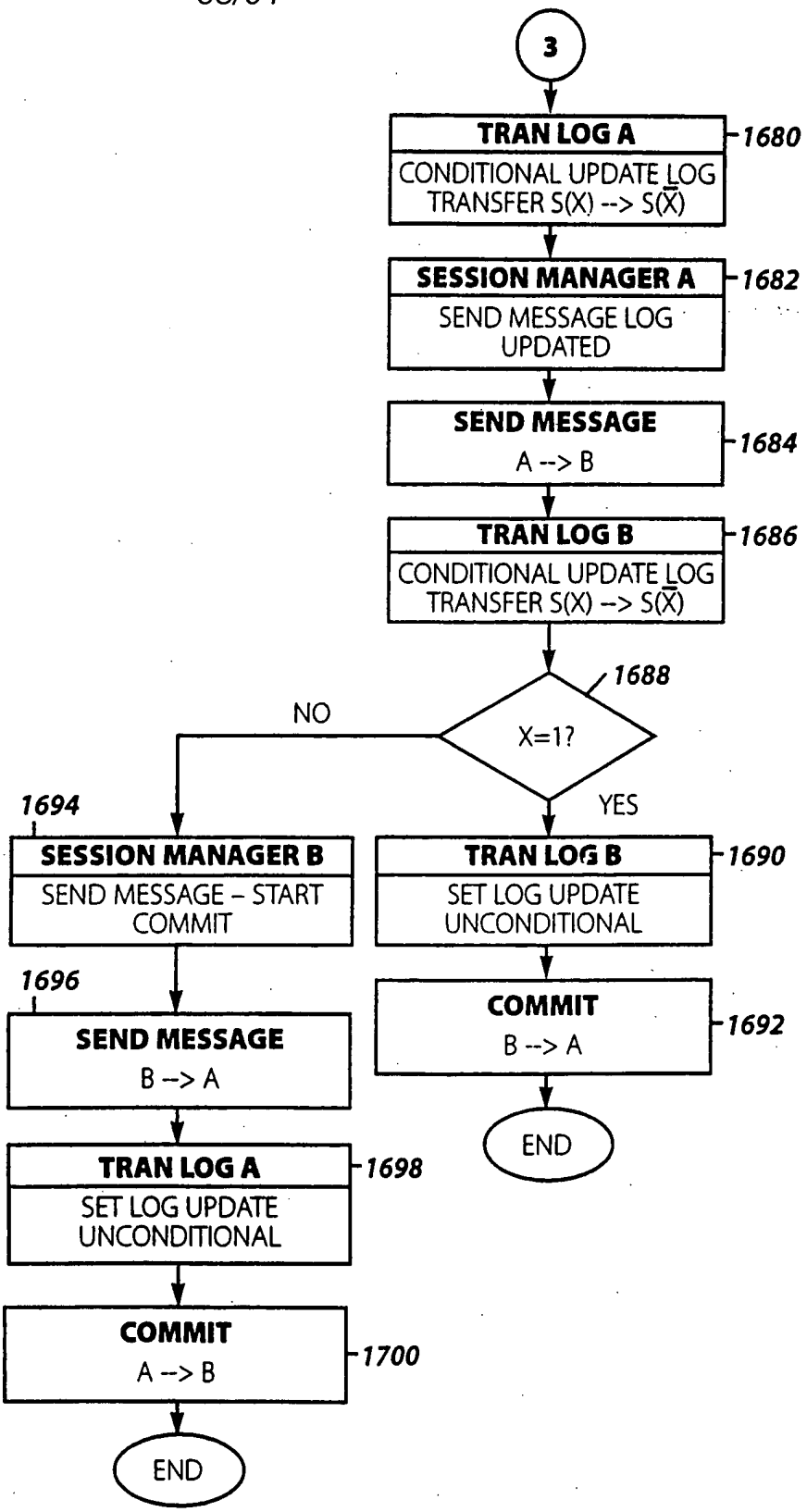
3
TRAN LOG A
CONDITIONAL UPDATE LOG
TRANSFER S(X) --> S(X̄)
1680
SESSION MANAGER A
SEND MESSAGE LOG
UPDATED
1682
SEND MESSAGE
A --> B
1684
TRAN LOG B
CONDITIONAL UPDATE LOG
TRANSFER S(X) --> S(X̄)
1686
1688
X=1?
NO
YES
1694
SESSION MANAGER B
SEND MESSAGE – START
COMMIT
1696
SEND MESSAGE
B --> A
TRAN LOG A
SET LOG UPDATE
UNCONDITIONAL
1698
COMMIT
A --> B
1700
END
TRAN LOG B
SET LOG UPDATE
UNCONDITIONAL
1690
COMMIT
B --> A
1692
END

Figure 40D

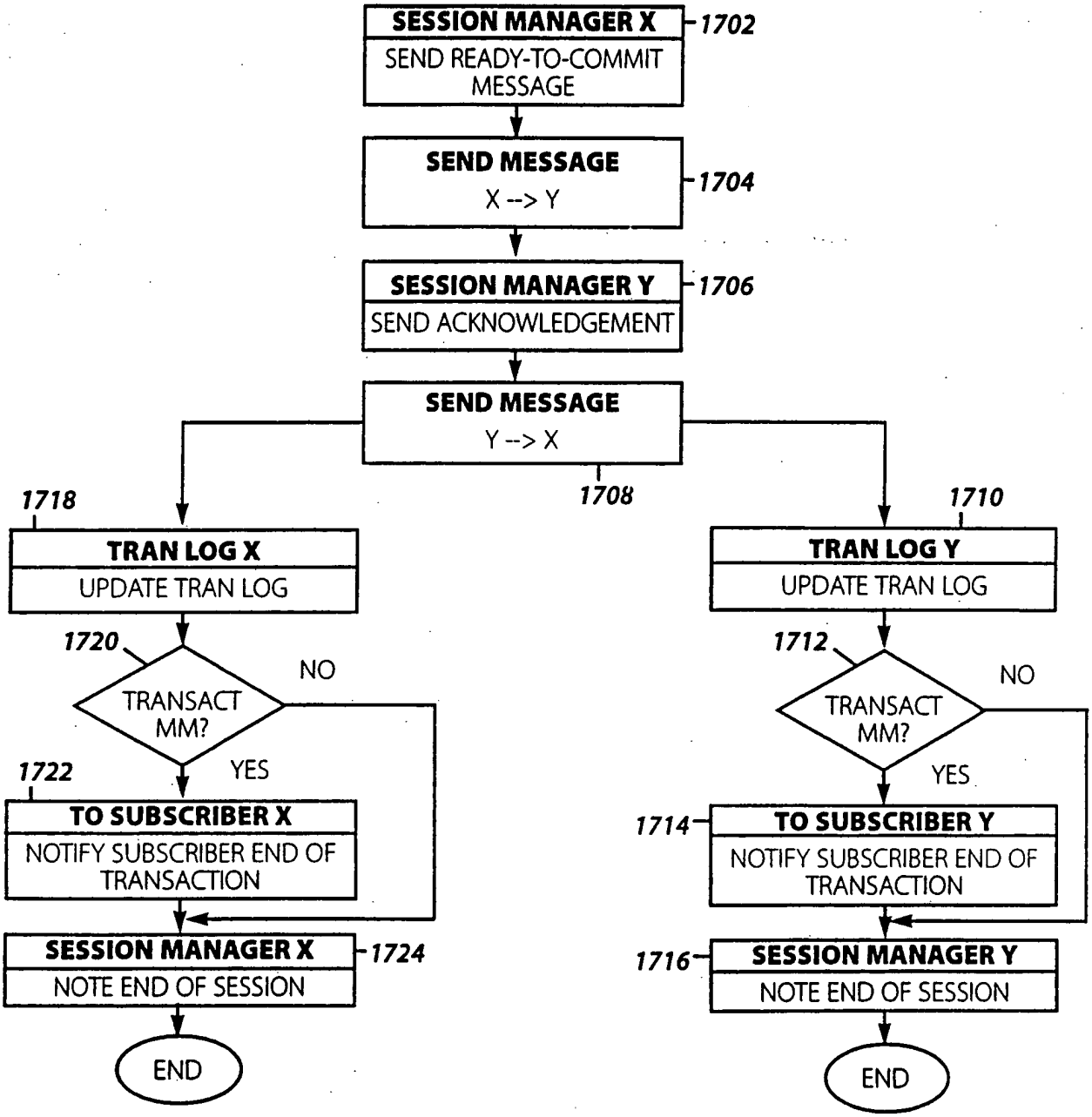
SESSION MANAGER X
SEND READY-TO-COMMIT MESSAGE
1702
SEND MESSAGE
X --> Y
1704
SESSION MANAGER Y
SEND ACKNOWLEDGEMENT
1706
SEND MESSAGE
Y --> X
1708
1718
TRAN LOG X
UPDATE TRAN LOG
1720
TRANSACT MM?
NO
YES
1722
TO SUBSCRIBER X
NOTIFY SUBSCRIBER END OF TRANSACTION
SESSION MANAGER X
NOTE END OF SESSION
1724
END
1710
TRAN LOG Y
UPDATE TRAN LOG
1712
TRANSACT MM?
NO
YES
1714
TO SUBSCRIBER Y
NOTIFY SUBSCRIBER END OF TRANSACTION
1716
SESSION MANAGER Y
NOTE END OF SESSION
END

Figure 41

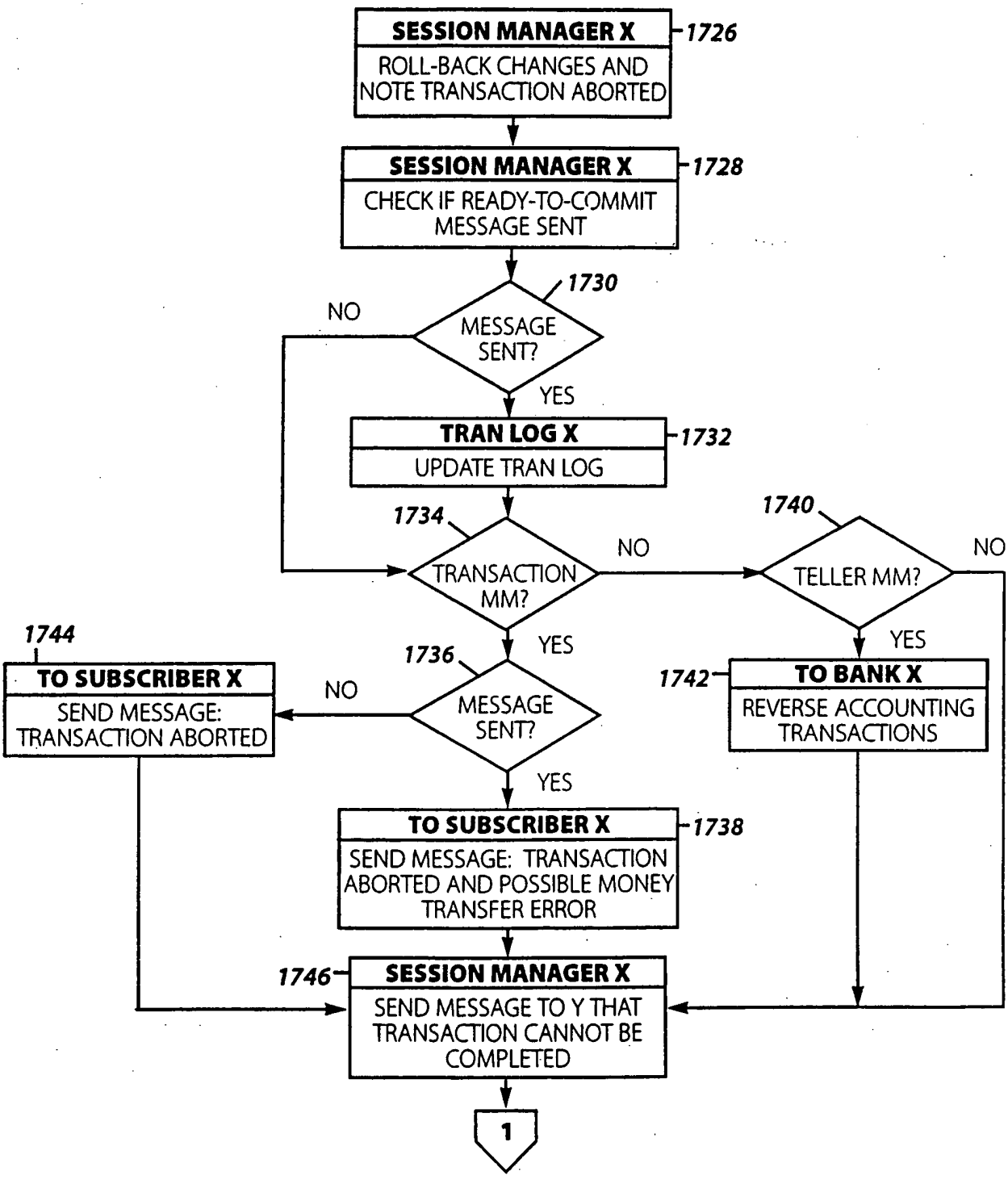
SESSION MANAGER X
1726
ROLL-BACK CHANGES AND NOTE TRANSACTION ABORTED
SESSION MANAGER X
1728
CHECK IF READY-TO-COMMIT MESSAGE SENT
1730
NO
MESSAGE SENT?
YES
TRAN LOG X
1732
UPDATE TRAN LOG
1734
TRANSACTION MM?
NO
1740
TELLER MM?
NO
YES
1744
TO SUBSCRIBER X
SEND MESSAGE: TRANSACTION ABORTED
1736
NO
MESSAGE SENT?
YES
1742
TO BANK X
REVERSE ACCOUNTING TRANSACTIONS
YES
TO SUBSCRIBER X
1738
SEND MESSAGE: TRANSACTION ABORTED AND POSSIBLE MONEY TRANSFER ERROR
1746
SESSION MANAGER X
SEND MESSAGE TO Y THAT TRANSACTION CANNOT BE COMPLETED
1

Figure 42A

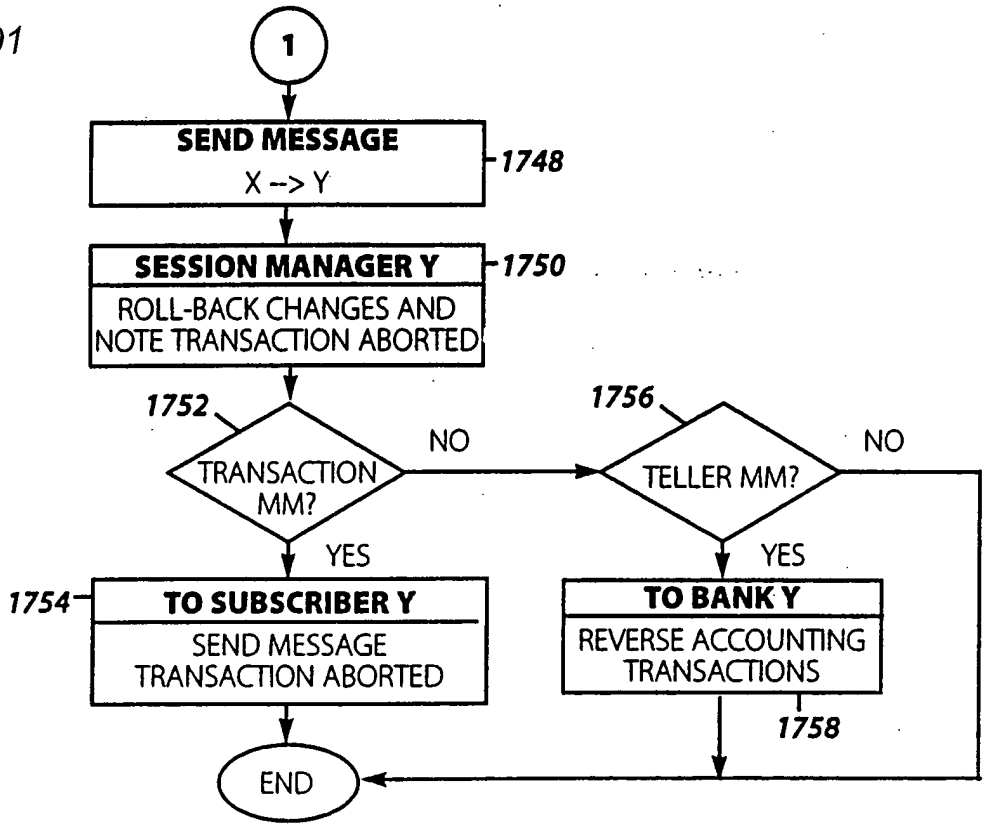
1
SEND MESSAGE
X --> Y
1748
SESSION MANAGER Y
ROLL-BACK CHANGES AND NOTE TRANSACTION ABORTED
1750
1752
TRANSACTION MM?
NO
1756
TELLER MM?
NO
YES
YES
1754
TO SUBSCRIBER Y
SEND MESSAGE TRANSACTION ABORTED
TO BANK Y
REVERSE ACCOUNTING TRANSACTIONS
1758
END

Figure 42B

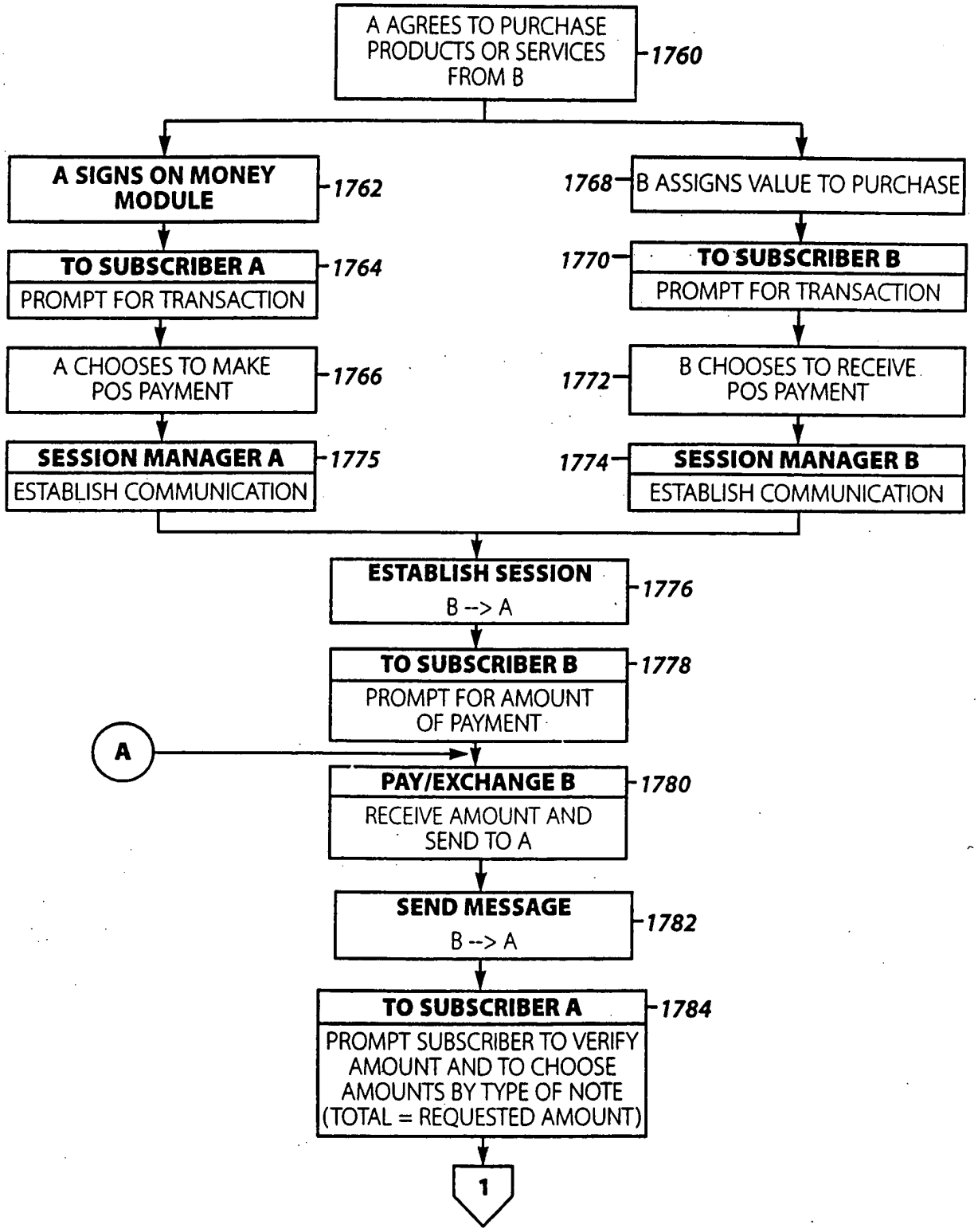
A AGREES TO PURCHASE PRODUCTS OR SERVICES FROM B
1760
A SIGNS ON MONEY MODULE
1762
TO SUBSCRIBER A
PROMPT FOR TRANSACTION
1764
A CHOOSES TO MAKE POS PAYMENT
1766
SESSION MANAGER A
ESTABLISH COMMUNICATION
1775
1768
B ASSIGNS VALUE TO PURCHASE
1770
TO SUBSCRIBER B
PROMPT FOR TRANSACTION
1772
B CHOOSES TO RECEIVE POS PAYMENT
1774
SESSION MANAGER B
ESTABLISH COMMUNICATION
ESTABLISH SESSION
B --> A
1776
TO SUBSCRIBER B
PROMPT FOR AMOUNT OF PAYMENT
1778
A
PAY/EXCHANGE B
RECEIVE AMOUNT AND SEND TO A
1780
SEND MESSAGE
B --> A
1782
TO SUBSCRIBER A
PROMPT SUBSCRIBER TO VERIFY AMOUNT AND TO CHOOSE AMOUNTS BY TYPE OF NOTE (TOTAL = REQUESTED AMOUNT)
1784
1

Figure 43A

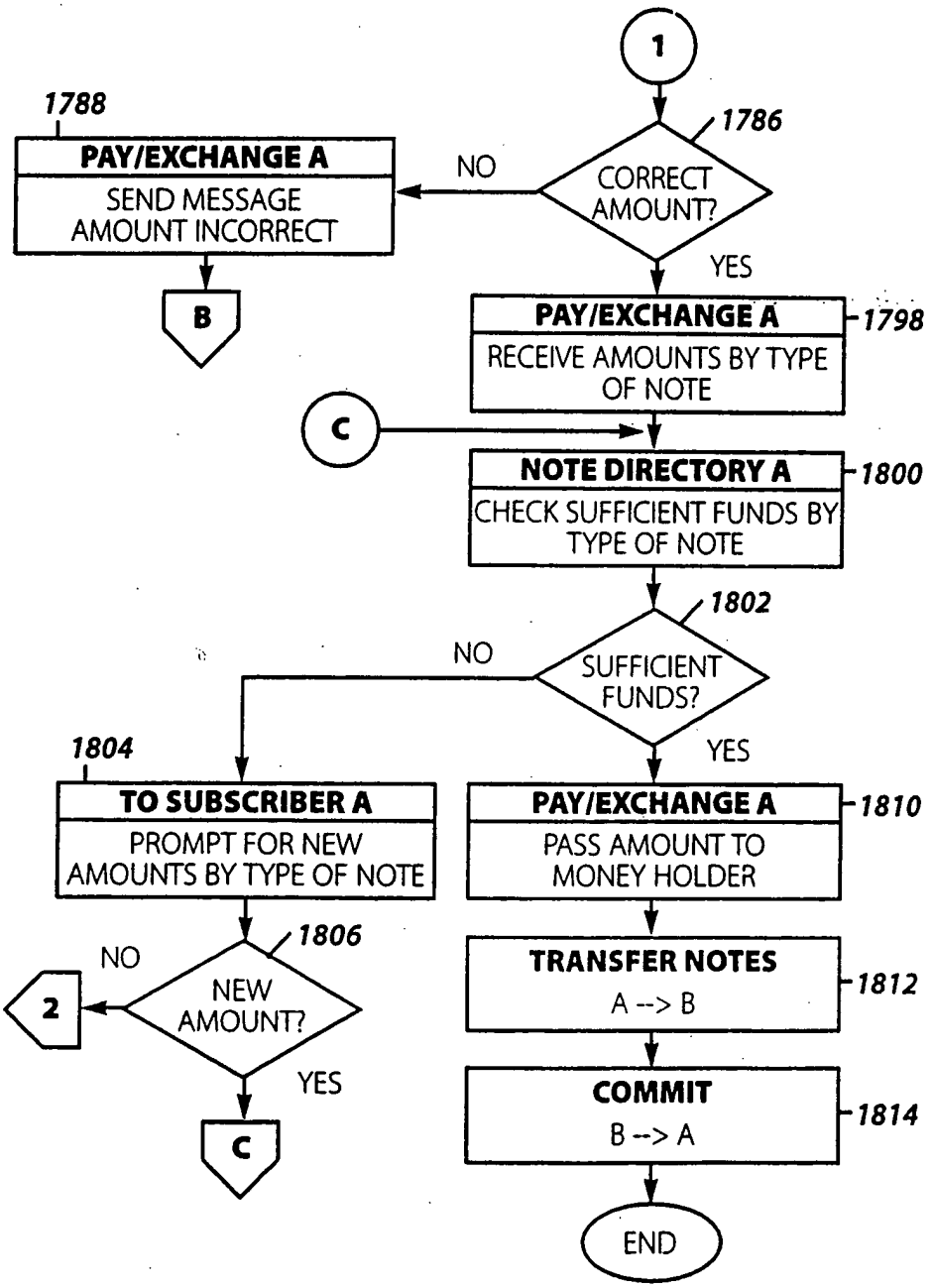
1
1786
CORRECT AMOUNT?
NO
1788
PAY/EXCHANGE A
SEND MESSAGE AMOUNT INCORRECT
B
YES
PAY/EXCHANGE A
RECEIVE AMOUNTS BY TYPE OF NOTE
1798
C
NOTE DIRECTORY A
CHECK SUFFICIENT FUNDS BY TYPE OF NOTE
1800
1802
SUFFICIENT FUNDS?
NO
YES
1804
TO SUBSCRIBER A
PROMPT FOR NEW AMOUNTS BY TYPE OF NOTE
PAY/EXCHANGE A
PASS AMOUNT TO MONEY HOLDER
1810
1806
NO
NEW AMOUNT?
2
YES
C
TRANSFER NOTES
A --> B
1812
COMMIT
B --> A
1814
END

Figure 43B

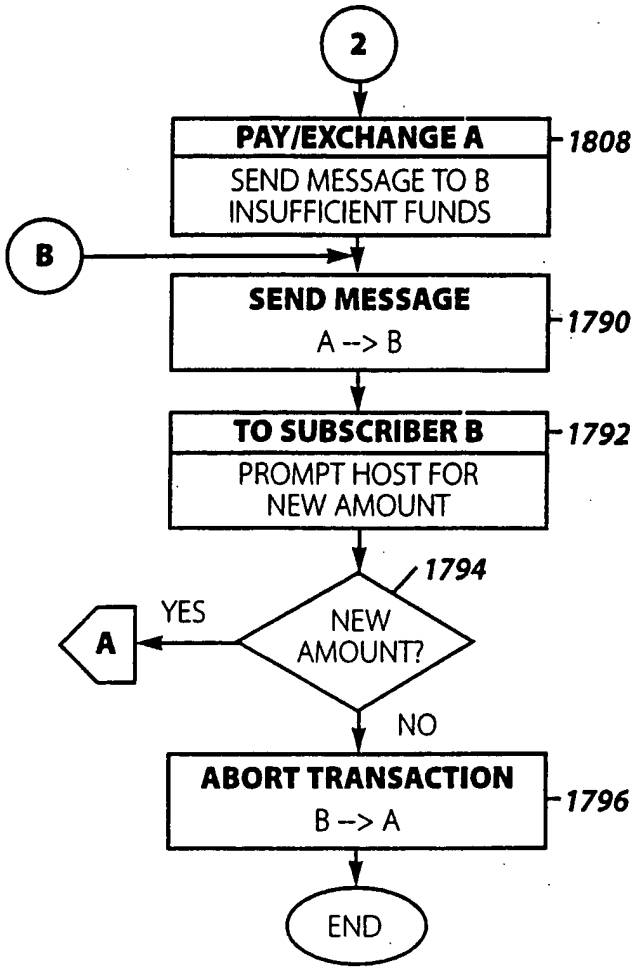
2
PAY/EXCHANGE A
SEND MESSAGE TO B
INSUFFICIENT FUNDS
1808
B
SEND MESSAGE
A --> B
1790
TO SUBSCRIBER B
PROMPT HOST FOR
NEW AMOUNT
1792
1794
YES
A
NEW
AMOUNT?
NO
ABORT TRANSACTION
B --> A
1796
END

Figure 43C

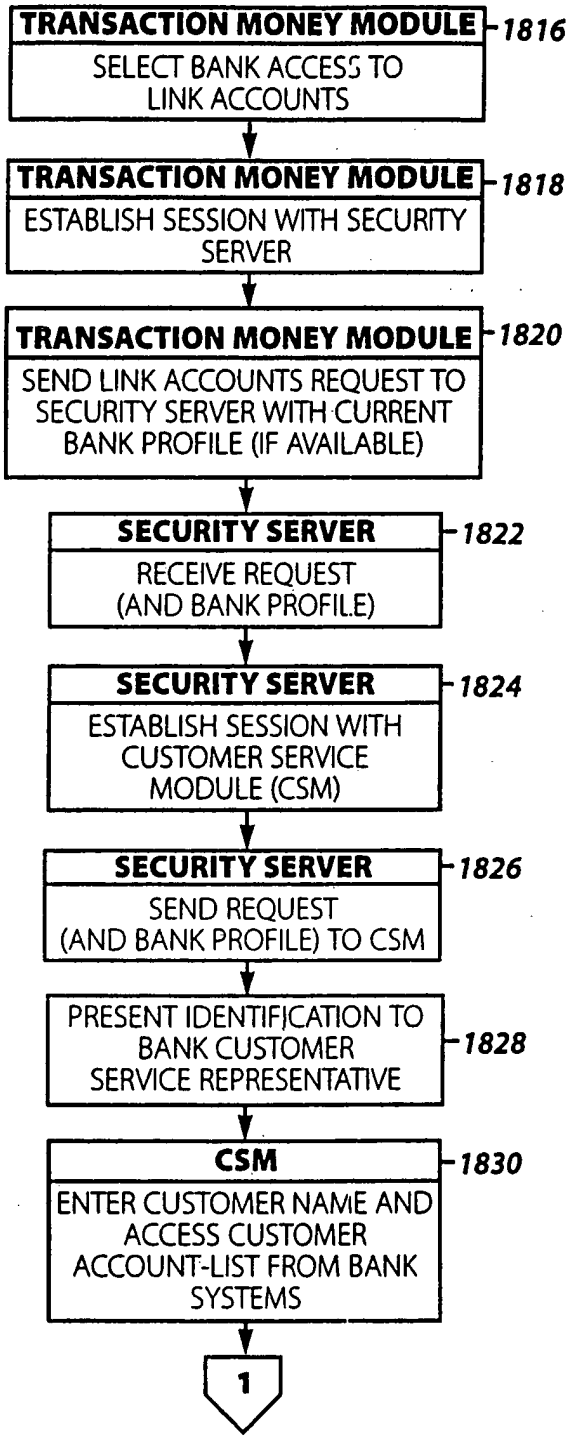
TRANSACTION MONEY MODULE
1816
SELECT BANK ACCESS TO LINK ACCOUNTS
TRANSACTION MONEY MODULE
1818
ESTABLISH SESSION WITH SECURITY SERVER
TRANSACTION MONEY MODULE
1820
SEND LINK ACCOUNTS REQUEST TO SECURITY SERVER WITH CURRENT BANK PROFILE (IF AVAILABLE)
SECURITY SERVER
1822
RECEIVE REQUEST (AND BANK PROFILE)
SECURITY SERVER
1824
ESTABLISH SESSION WITH CUSTOMER SERVICE MODULE (CSM)
SECURITY SERVER
1826
SEND REQUEST (AND BANK PROFILE) TO CSM
PRESENT IDENTIFICATION TO BANK CUSTOMER SERVICE REPRESENTATIVE
1828
CSM
1830
ENTER CUSTOMER NAME AND ACCESS CUSTOMER ACCOUNT-LIST FROM BANK SYSTEMS
1

Figure 44A

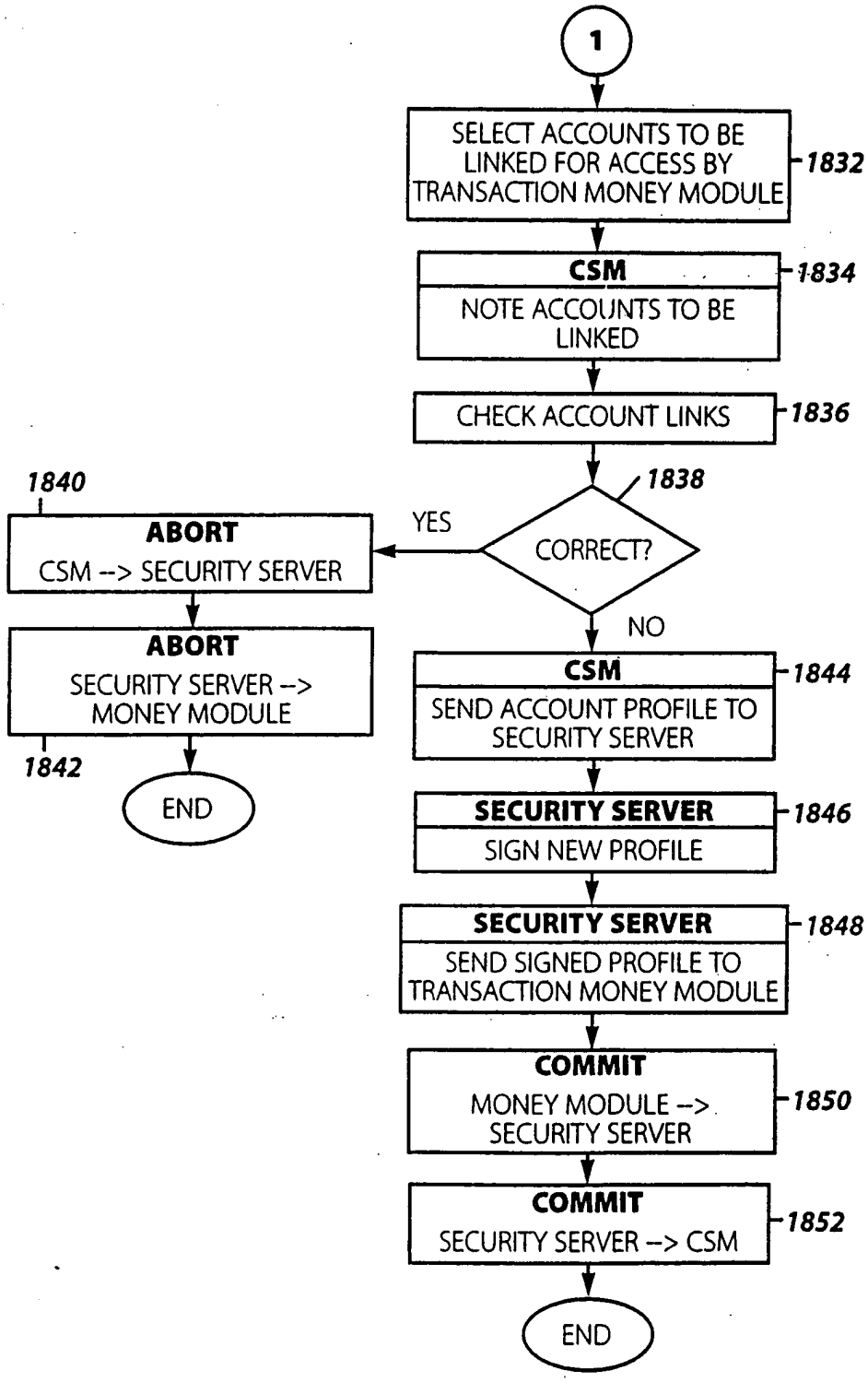
1
SELECT ACCOUNTS TO BE LINKED FOR ACCESS BY TRANSACTION MONEY MODULE
1832
CSM
NOTE ACCOUNTS TO BE LINKED
1834
CHECK ACCOUNT LINKS
1836
1838
CORRECT?
YES
NO
1840
ABORT
CSM --> SECURITY SERVER
ABORT
SECURITY SERVER --> MONEY MODULE
1842
END
CSM
SEND ACCOUNT PROFILE TO SECURITY SERVER
1844
SECURITY SERVER
SIGN NEW PROFILE
1846
SECURITY SERVER
SEND SIGNED PROFILE TO TRANSACTION MONEY MODULE
1848
COMMIT
MONEY MODULE --> SECURITY SERVER
1850
COMMIT
SECURITY SERVER --> CSM
1852
END

Figure 44B